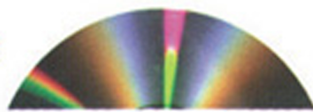
Microsoft® Official Study Guide





CD-ROM includes:
- **Windows 2000 Advanced Server** Evaluation Software 120 day limit on use
- Exercises with Practice Files



Microsoft®



MCSE

self-paced exams

knowledge educate empower

hands-on training

IT Professional



Microsoft® Certified Professional

MCSE Study Guide for Exam 70-215

ייעוץ מקצועי:

נגה קרטס

Microsoft Certified Professional Trainer

שלום נחייסי

Microsoft Certified Professional System Trainer

Microsoft® Windows® 2000 Server

הכנה למבחן הסמכה

Microsoft®

MCSE Training Kit

Microsoft®

Windows® 2000 Server

הכנה למבחן הסמכה

#70-215

קרא על התקליטור בהקדמה
ובקובץ ONCD שבתקליטור

עורכים : **צור ריכטר-לוין**  , **זהר עמיהוד** 

ייעוץ מקצועי : **שלום נחייסי**  
ראש תחום רשתות בחברת הדרכה

נגה קרטס 

מתרגמים : **צור ריכטר-לוין**  **, יואב הופמן, גלית איטקין**

עריכה ועיצוב : **שרה עמיהוד, ענבל אילני**

עיצוב עטיפה : **ישראל מצגר**

שמות מסחריים

הודעה

לשם שטף הקריאה כתוב ספר זה בלשון זכר בלבד. ספר זה מיועד לגברים ונשים כאחד ואין בכוונתנו להפלות או לפגוע בציבור המשתמשים/ות.

- ❑ **טלפון: 09-9564716**
- ❑ **פקס: 09-9571582**
- ❑ **דואר אלקטרוני** : **info@hod-ami.co.il**
- ❑ **אתר באינטרנט** : **www.hod-ami.co.il**

Microsoft®

MCSE Training Kit

Microsoft® Windows® 2000 Server

הכנה למבחן הסמכה

#70-215

Microsoft®



MCSE Training Kit Microsoft Windows 2000 Server

By Microsoft Corporation

הוצאת הוד-עמי לספרי מחשבים בע"מ

ת.ד. 6108 הרצליה 46160

טלפון: 09-9564716 פקס: 09-9571582

www.hod-ami.co.il

info@hod-ami.co.il

מהדורה ראשונה 2000

הדפסה שנייה ומעודכנת 2001, 2002

HOD-AMI Ltd.
P.O.B. 6108, Herzliya
ISRAEL, 2000

ISBN 965-361-249-2 מסת"ב

תוכן עניינים מקוצר

נספחים

תוכן העניינים

פרק 3: התקנות אוטומטיות של Windows 2000 Server 97

פרק 4: מערכת הקבצים של Windows 2000 147

פרק 13: ניטור ומיטוב 761

אודות ספר זה

ברוכים הבאים לערכת ההדרכה לבחינת הסמכה 70-215 מבית Microsoft Press.

MCSE Training Kit-Microsoft Windows 2000 Server

ערכת הדרכה זו תדריך אותך כיצד להתקין ולהגדיר את Windows 2000 Server. ותכשיר אותך לקראת הבחינה שמספרה 70-215 בדרך לקבלת תואר MCSE.

למה ללמוד בעברית כשהבחינה באנגלית?

אכן, בחינות ההסמכה של Microsoft נערכות באנגלית. גם חומר הלימוד המחולק במרכזי ההדרכה המורשים של Microsoft הוא באנגלית, ובכל זאת יש מקום לספר לימוד בעברית. הכיצד?

❖ המונחים שבספר מופיעים באנגלית ולידם הסבר בעברית.

❖ השאלות בסוף כל פרק הן באנגלית וגם בעברית.

❖ מילון המונחים, Glossary, הוא באנגלית.

❖ האינדקס הענק, בעזרתו תוכל למצוא כל דבר, הוא באנגלית.

תהליך הלימוד

לאחר מבוא קצר לתכונות של כל מהדורות Windows 2000, תלמד כיצד להתקין את Windows 2000 Server באמצעות שגרות התקנה ידניות ואוטומטיות. לאחר ההתקנה, תלמד על שיטות הקבצים השונות (FAT32 ,FAT16 ,NTFS) ופעולות ניהול דיסקים הזמינות במערכת Windows 2000 Server. בהמשך נחקור את ניהול מערכת ההפעלה ואת מכלול Active Directory Services, שהם הכרחיים להבנת Windows 2000. בנוסף, תלמד על פרוטוקולים של רשת, ניתוב וגישה מרחוק ופעולות יישומי שרת נוספות, כגון שירותי מסופים (Terminal Services). לבסוף, נדון בניטור ומיטוב Windows 2000 Server.

כל פרק בספר זה מחולק לשיעורים. שיעורים רבים כוללים הליכים מעשיים המאפשרים תרגול או הדגמת המושג או הצגת היכולת. כל פרק מסתיים בסיכום קצר של כל השיעורים בפרק, ושאלות סיכום לבחינת שליטתך בחומר שנלמד בפרק.

סעיף "התחלת הקורס" במבוא זה מספק הוראות התקנה חשובות, המתארות את החומרה והתוכנה הנדרשות להשלמת ההליכים בקורס זה. כמו כן הוא כולל מידע אודות תצורת הרשת הנדרשת להשלמת חלק מההליכים המעשיים. קרא חלק זה בעיון לפני התחלת השיעורים.

למי מיועד הספר?

ספר זה פותח לשני קהלי יעד:

- ❖ אנשי מקצוע בתחום טכנולוגיית המידע **I**nformation **T**echnology (IT), הנדרשים לתכנן, ליישם ולתמוך במערכת Windows 2000 Server,
- ❖ למתכוונים להיבחן בבחינה 70-215 של Microsoft:

Microsoft Certified Professional exam 70-215: Installing, Configuring, and Administrating Microsoft 2000 Server.

דרישות מקדימות

הדרישות המקדימות לקורס זה הן:

- ❖ ידע עדכני ביסודות טכנולוגיות רשת.
- ❖ יכולת התמצאות בממשק מערכת ההפעלה של Windows (במיוחד ממשקי Windows 95, Windows 98, Windows NT או Windows 2000).
- ❖ מומלצים לפחות ששה חודשי ניסיון בתמיכת רשתות, או סיום בהצלחה של הקורס Networking Essentials, Hands-On Self Paced Training (או קורס מקביל לו) לתמיכה ברשתות תקשורת מקומיות ורחבות.
- ❖ ניסיון בפקודות מערכת הפעלה חיצוניות ופנימיות בסיסיות כגון: CD, Dir, Fdisk ו-Format.
- ❖ ידע מעשי בגישה ושינוי הגדרות BIOS במחשבים.
- ❖ הדרכה קודמת או ידע על Microsoft Windows 2000 Professional.
- ❖ לא נדרשת הדרכה קודמת או ידע ב- Windows NT Server, אך הדבר יכול לסייע בתהליך הלמידה.

חומר עיוני

חומר העיון הבא עשוי להיות שימושי:

- ❖ MCP Magazine Online, באתר: http://www.mcpmag.com
- ❖ אתר האינטרנט של Microsoft (http://www.microsoft.com) ו-Microsoft TechNet Technical Plus, הזמין על תקליטור חודשי ובאתר Microsoft.
- ❖ Microsoft Windows 2000 Server Resource Kit, הוצאת Microsoft, 1999.
- ❖ MCSE Training Kit - Microsoft Windows 2000 Professional, הוצאת Microsoft, 2000.
- ❖ MCSE, הכנה למבחן הסמכה Networking Essentials exam 70-058, מהדורה שלישית, הוצאת הוד-עמי, 2000.
- ❖ Operating System Concepts מאת Silberschatz A. ו-P.Galvin, מהדורה חמישית, הוצאת Addison-Wesley, 1998.
- ❖ Windows NT Magazine (שייקרא בקרוב Windows 2000 magazine). חוברת מקוונת זו נמצאת באתר http://www.winntmag.com והיא יוצאת לאור על ידי Duke Communications.
- ❖ אתר Sysinternals Freeware ב- http://www.sysinternals.com.

אודות התקליטור המצורף

התיקיה הרלוונטית לספר זה היא **X:\Books\59279** בה נמצאים תיקיות משנה לפי חלוקת הפרקים. תמצא בה מיגוון עזרי מידע, הניתנים לשימוש לכל אורך הספר. זה כולל קבצים, נספחים ומאמרים, המשמשים בתרגילים מעשיים. ניתן להשתמש בקבצים אלה ישירות מהתקליטור או להעתיקם לדיסק הקשיח. למידע נוסף על תכולה ושימוש ראה ReadmeH.txt בתיקיה (לחץ לחיצה כפולה כדי לפתוח אותו).

כמו כן מכיל התקליטור המצורף **גרסת ניסיון - Windows 2000 Server**, גירסה המוגבלת ל-120 יום. זוהי גירסה מלאה המאפשרת ביצוע כל המשימות בהן דן הספר.

תוכנית ההתקנה של Windows 2000 Server בגרסת Evaluation המצורפת בתקליטור מתחילה באופן אוטומטי עם טעינת התקליטור לכונן התקליטורים.

קרא את ההוראות המפורטות שבקובץ ONCD שבתקליטור **לפני תחילת ההתקנה!!!**

מומלץ להתקין גירסה זו במחשב ייעודי.

דרישות החומרה המינימליות להתקנה הן: מחשב עם מעבד פנטיום 133 מגה-הרץ לפחות, 128 מגה-בית זיכרון RAM ולפחות 2 ג'יגה-בית פנויים בכונן הדיסק הקשיח.

מבנה הספר

כל פרק פותח בסעיף "לפני שתתחיל", המכין אותך להמשך הפרק.

הפרקים בנויים משיעורים. שיעורים רבים כוללים תרגילים הנותנים לך הזדמנות להשתמש ביכולות שהוצגו, או לחקור את חלק היישום שתואר. כל התרגילים בנויים מהליכים שלב-אחר-שלב המזוהים על ידי הכותרת "הליך...".

הסעיף "שאלות סיכום" בסוף כל פרק מאפשר לך לבחון מה למדת בשיעורי הפרק.

נספח A מכיל את כל שאלות הפרק והתשובות המתאימות באנגלית.

הערות

מספר סוגי הערות מופיעים בשיעורים:

- **טיפ** - כולל הסברים לתוצאות אפשריות או שיטות חליפיות.
- **חשוב** - כולל מידע חיוני להשלמת המטלה.
- **הערה** - כולל מידע נוסף והפניות.
- **אזהרה** - כולל אזהרות על אפשרות אובדן נתונים.

מוסכמות

המוסכמות הבאות משמשות בספר כולו.

מוסכמות כתיבה

- תווים או פקודות להקלדה מופיעים בכתב **מודגש (Bold).**
- שמות תיקיות וקבצים מופיעים בלועזית, כאשר האות הראשונה היא אות רישית (גדולה), פרט למקרים בהם אתה אמור להקליד אותם ישירות. אלא אם צוין אחרת, ניתן להשתמש באותיות קטנות להקלדת שם קובץ בתיבת דו-שיח או בשורת הפקודות.
- סיומות שמות קבצים מופיעות כולן באות קטנה.
- ראשי תיבות מופיעים באות גדולה.
- סוגריים משולשים < > משמשים בפסוקי תחביר לתחום פריט אופציונלי. לדוגמה, <*filename*> בתחביר פקודה מציין שניתן להקליד שם קובץ עם הפקודה. הקלד רק את הנתון שבתוך הסוגריים, לא את הסוגריים עצמם.

מוסכמות מקלדת

- ❖ סימן חיבור (+) בין שני שמות מקשים, מורה שעליך ללחוץ על שניהם בו-זמנית. לדוגמה, "לחץ Alt+Tab" משמעו שעליך ללחוץ על Alt ולהשאירו לחוץ בעודך לוחץ על Tab.
- ❖ פסיק (,) בין שני שמות מקשים או יותר, משמעו שעליך ללחוץ על כל מקש ברצף ולא יחדיו. לדוגמה "לחץ Alt, F, X", משמעו שעליך ללחוץ ולשחרר כל מקש לפי תור. "לחץ Alt+W, L, משמעו שעליך קודם ללחוץ על Alt ו-W ביחד, לשחררם וללחוץ על L.
- ❖ תוכל לבחור פקודות תפריט באמצעות המקלדת. לחץ על מקש Alt להפעלת סרגל התפריטים, ואז בחר ולחץ לפי סדר את המקשים המתאימים לאות המוארת/מודגשת או אות עם קו תחתי המציינים את שם התפריט ושם הפקודה. עבור כמה פקודות תוכל גם ללחוץ על שילוב מקשים המפורט בתפריט.
- ❖ ניתן לבחור או לבטל בחירה מתיבות סימון או לחצני אפשרויות בתיבות דו-שיח באמצעות המקלדת. לחץ על מקש Alt, ולחץ על המקש המתאים לאות בעלת הקו התחתי של שם האפשרות. לחליפין, תוכל ללחוץ על Tab עד שהאפשרות תואר, ואז ללחוץ על מקש הרווח כדי לבחור או לבטל בחירה מתיבת הסימון או מלחצן האפשרויות.
- ❖ ניתן לבטל את תצוגת תיבת הדו-שיח על ידי לחיצה על מקש Esc.

סקירת פרקים ונספחים

קורס בקצב-אישי זה משלב טקסט תיאורי, הערות, הליכים מעשיים ושאלות סיכום, ללמדך להתקין ולהגדיר את Windows 2000 Server. הוא תוכנן לביצוע מההתחלה עד הסוף, אך תוכל לבחור מסלול לימוד אישי ולהשלים רק את החלקים המעניינים אותך (ראה בסעיף הבא, "מציאת נקודת ההתחלה הטובה ביותר עבורך", מידע נוסף). אם תבחר את אפשרות מסלול הלימוד האישי, עיין בסעיף "לפני שתתחיל" בכל פרק. בכל הליך מעשי הדורש פעולות מקדימות מפרקים קודמים, עיין בפרקים המתאימים.

הספר מחולק לפרקים הבאים:

- ❖ חלק "אודות ספר זה" מכיל סקירת הדרכה בקצב-אישי, ומציג את רכיבי ההדרכה. קרא חלק זה בעיון לקבלת ערך לימודי מירבי מהדרכה זו וכדי לתכנן איזה פרקים תלמד. חיוני להיצמד למידע ההתקנה המפורט ב"אודות ספר זה" להשלמה מוצלחת של התרגילים בערכת ההדרכה.
- ❖ פרק 1, "מבוא ל-Windows 2000", מסכם את תכונות Windows 2000, מבנה מערכת ההפעלה ושירותי המדריך של Windows 2000.
- ❖ פרק 2, "התקנה והגדרה של Windows 2000 Server", מכסה את אופן ההכנה, ההתקנה, השדרוג ואיתור תקלות בהתקנה של Windows 2000 Server.

- פרק 3, "התקנות אוטומטיות של Windows 2000 Server", דן בדרך ההכנה וביצוע של התקנה אוטומטית של Windows 2000 Server ויישומי שרת.
- פרק 4, "מערכת הקבצים של Windows 2000" בוחן יסודות ניהול דיסקים, מערכות קבצים של Windows 2000, ואבטחת מערכת הקבצים.
- פרק 5, "מערכות קבצים מתקדמות", חוקר את Distributed File System ושירות שכפול קבצים.
- פרק 6 "Active Directory Services", מתאר כיצד לתכנן, ליישם ולנהל את שירותי Active Directory.
- פרק 7 "ניהול שרת Windows 2000", מכסה את אופן השימוש ב-MMC (מערכת MMC כוללת ממשק משתמש וכלי תצוגה אחיד המאפשר שילוב של כל ריכיבי הניהול), לניהול חשבונות משתמשים וקבוצות ולהחלת מדיניות קבוצה.
- פרק 8, "ניהול שירותי הדפסה", מספק סקירה של נושא ההדפסה ב-Windows 2000, כולל כיצד להתקין, לנהל ולחבר מדפסת רשת. פרק זה גם סוקר את הקשר שבין שירותי Active Directory להדפסה.
- פרק 9, "פרוטוקולי רשת ושירותים", מציג פרוטוקולים של רשתות, ומספק פרטים על TCP/IP, DHCP, WINS ו-DNS.
- פרק 10, "שירות ניתוב וגישה מרחוק (Routing and Remote Access Service)", מכסה את תכונות הניתוב וגישה מרחוק, כולל התקנת RAS ו-VPN וכיצד להשתמש בכלי RRAS.
- פרק 11, "אמצעי אבטחת מידע בסביבת Windows 2000", בוחן את PKI, טכנולוגיות מפתח ציבורי ו-Kerberos ב-Windows 2000. הפרק גם דן בכלי הגדרות אבטחה ויישום בקרה ב-Windows 2000.
- פרק 12, "אמינות וזמינות", דן בניהול התקני חומרה ומנהלי התקנים, יישום גיבוי של Windows 2000, בניית אסטרטגיית הגנה בפני אסון והתאוששות מאסון.
- פרק 13, "ניטור ומיטוב" מתאר ניטור ומיטוב של ביצועי Windows 2000, סוקר את SNMP, ודן באופן השימוש בעמדת ביצועים, ניתור רשת ומנהל מטלות.
- פרק 14, "שרתי יישומים של Windows 2000" דן בהתקנה ובהגדרה של Internet Information Services 5.0, שירותי Telnet ושירותי מסופים.
- נספח A "Questions and Answers", מהווה רשימה של כל השאלות בסעיפי "שאלות סיכום" בספר, עם התשובות.
- נספח B "Sample Answer Files for Unattended Setup", מספק מידע על יצירת קובץ התקנה להתקנה לא מאוישת.
- נספח C "Installing Service Packs", מספק מידע על התקנה וניהול ערכות שירות ב-Windows 2000.

❖ ה-Glossary כולל מונחים חשובים באנגלית ופירוט על כל מונח.

❖ אינדקס מפורט ביותר באנגלית.

מציאת נקודת ההתחלה הטובה ביותר עבורך

כיון שספר זה נועד להדרכה בקצב-אישי, תוכל לדלג על כמה שיעורים ולשוב אליהם מאוחר יותר. אולם, שים לב שבמקרים רבים, עליך להשלים תרגילים בכל פרק לפני השלמת תרגילים בפרקים מאוחרים יותר. השתמש בטבלה הבאה למציאת נקודת ההתחלה הטובה ביותר עבורך.

אם אתה	עקוב אחר מסלול הלימוד הזה
מתכוון לגשת למבחן 70-210: Microsoft Certified Professional, מבחן 70-215: התקנה, הגדרה, וניהול Windows 2000 Server של Microsoft.	קרא את סעיף "התחלת הקורס". למד את פרקים 1 ו- 2. למד את שאר הפרקים בסדר כלשהו. קרא בעיון את סעיפי "לפני שתתחיל" בכל פרק כדי לקבוע את התלות בביצוע תרגילים מפרקים קודמים.
מעיין במידע על נושאים מסוימים מהבחינה.	השתמש בטבלאות שבהמשך.

Installing Windows 2000 Server

Skills Being Measured	Chapter	Lesson
Perform an attended installation of Windows 2000 Server.	2	1-2
Perform an unattended installation of Windows 2000 Server. • Create unattended answer files by using Setup Manager to automate the installation of Windows 2000 Server. • Create and configure automated methods for installation of Windows 2000.	3	1-3
Upgrade a server from Microsoft Windows NT 4.0.	2	3
Deploy service packs.	12	1
Troubleshoot failed installations.	2	4

Installing, Configuring, and Troubleshooting Access to Resources

Skills Being Measured	Chapter	Lesson
Install and configure network services for interoperability.	14 9	1-4 3-5
Monitor, configure, troubleshoot, and control access to printers.	8	2-5
Monitor, configure, troubleshoot, and control access to files, folders, and shared folders.	4 5 14	1-4 1-2 1-2
Configure, manage, and troubleshoot a stand- alone Distributed file system (Dfs) .	5	1
Configure, manage, and troubleshoot a domain- based Distributed file system (Dfs).	5 6	1 3
Monitor, configure, troubleshoot, and control local security on files and folders.	4	4
Monitor, configure, troubleshoot, and control access to files and folders in a shared folder.	4	4
Monitor, configure, troubleshoot, and control access to files and folders via Web services.	14	1-2
Monitor, configure, troubleshoot, and control access to Web sites.	14	1-2

Configuring and Troubleshooting Hardware Devices and Drivers

Skills Being Measured	Chapter	Lesson
Configure hardware devices.	12	1
Configure driver signing options.	12	1
Update device drivers.	12	1
Troubleshoot problems with hardware.	12	1

Managing, Monitoring, and Optimizing System Performance, Reliability, and Availability

Skills Being Measured	Chapter	Lesson
Monitor and optimize usage of system resources.	13	2-5
Manage processes. • Set priorities, and start and stop processes.	13 13	5 5
Optimize disk performance.	13	1
Manage and optimize availability of system state data and user data.	12	1-4
Recover systems and user data. • Recover systems and user data by using Windows Backup. • Troubleshoot system restoration by using Safe Mode. • Recover systems and user data by using the Recovery Console.	12 12 12 12	2, 4 2, 4 4 4

Managing, Configuring, and Troubleshooting Storage Use

Skills Being Measured	Chapter	Lesson
Configure and manage user profiles.	7	2
Monitor, configure, and troubleshoot disks and volumes.	12 13	3 1
Configure data compression.	13	1
Monitor and configure disk quotas.	13	1
Recover from disk failures.	12	4

Configuring and Troubleshooting Windows 2000 Network Connections

Skills Being Measured	Chapter	Lesson
Install, configure, and troubleshoot shared access.	4	4
Install, configure, and troubleshoot a virtual private network (VPN).	10	4
Install, configure, and troubleshoot network protocols.	9	1, 2
Install and configure network services.	9 13	3-5 4

Skills Being Measured	Chapter	Lesson
Configure, monitor, and troubleshoot remote access.	10	1-3, 5
• Configure inbound connections.	10	1-3
• Create a remote access policy.	10	3
• Configure a remote access profile.	10	1-3
Install, configure, monitor, and troubleshoot Terminal Services.	14	4
• Remotely administer servers by using Terminal Services.	14	4
• Configure Terminal Services for application sharing.	14	4
• Configure applications for use with Terminal Services.	14	4
Configure the properties of a connection.	2 9 10	2 2-5 3, 4
Install, configure, and troubleshoot network adapters and drivers.	2 9 12	1, 2 2 1

Implementing, Monitoring, and Troubleshooting Security

Skills Being Measured	Chapter	Lesson
Encrypt data on a hard disk by using Encrypting File System (EFS) .	11	2
Implement, configure, manage, and troubleshoot policies in a Windows 2000 environment.	7	4
• Implement, configure, manage, and troubleshoot Local Policy in a Windows 2000 environment.	7	4
• Implement, configure, manage, and troubleshoot System Policy in a Windows 2000 environment.	7	4
Implement, configure, manage, and troubleshoot auditing.	11	5
Implement, configure, manage, and troubleshot local accounts.	7	2
Implement, configure, manage, and troubleshoot Account Policy.	7	2, 4
Implement, configure, manage, and troubleshoot security by using the Security Configuration Tool Set.	11	4

תרגול

קורס הדרכה זה כולל הליכים מעשיים המסייעים בהבנת Windows 2000 Server.

להשלמת חלק מהליכים אלה, נדרשים שני מחשבים מחוברים ברשת, או חיבור לרשת גדולה יותר. המצב המיטבי הוא שהרשת המשמשת לתרגילים בערכה זו, לא תהיה רשת מבודדת. שני המחשבים צריכים להיות בעלי יכולת הפעלת Windows 2000 Server.

אזהרה מספר תרגילים עשויים לדרוש ממך לבצע שינויים בשרתים. לכך עלולות להיות תוצאות בלתי רצויות אם אתה מחובר לרשת גדולה. בדוק ותאם עם מנהל הרשת, לפני ביצוע תרגילים אלה.

המחשב הראשון ייקרא Computer1 עם שם מחשב Server01. המחשב השני ייקרא Computer2 עם שם מחשב Server02. שני המחשבים יהיו בעלי יכולת הפעלת Windows 2000 Server. אם יש לך רק מחשב אחד, קרא את השלבים והכר את ההליכים לפי מיטב יכולתך. Computer1 ו-Computer2 מתוארים ביתר פירוט בסעיף "הוראות התקנה" של מסמך זה.

הפעלה של הסברים והליכים נעשית דרך רכיבי ממשק Windows, כגון **M**icrosoft **M**anagement **C**onsole - **MMC** ניתן לגשת לאובייקטים רבים המופיעים בממשק Windows דרך תפריטי קיצור. אם אתה משתמש בהגדרות עכבר ימניות, הגישה לתפריטי הקיצור היא על ידי הצבעה על אובייקט ולחיצה ימנית על העכבר. אם אתה משתמש בהגדרות עכבר שמאליות, תפריטי הקיצור נגישים על ידי הצבעה על אובייקט ולחיצה שמאלית על העכבר.

דרישות חומרה מינימליות

על כל מחשב להיות בעל תצורת החומרה המינימלית הבאה (כדי שתצליח לסיים, עוד השנה, את ההליכים רצוי שתשיג לך מחשב(ים) "חזקים" הרבה יותר. למשל, אם ההמלצה היא Pentium 133Mhz השג לך Pentium 600Mhz ומעלה). כל החומרה צריכה להיכלל ברשימת Microsoft לתאימות עם Windows 2000 Server (רשימת HCL).

- Pentium 133Hhz
- 128MB זיכרון RAM
- 2GB שטח פנוי למחיצת אתחול (המחיצה המכילה את קבצי מערכת ההפעלה) וקבצים אחרים הנוצרים במהלך התרגילים בקורס זה.
- 500MB שטח לא מוקצה על המחשב שיהיה Server01 במהלך ביצוע התרגילים בערכה זו (השטח הלא מוקצה יחצץ בתרגילים בפרק 4).
- כונן תקליטורים במהירות 12x.

- מסך VGA (מומלצת הפרדה של לפחות 800 x 600).
- עכבר Microsoft או התקן הצבעה תואם.
- מודם במחשב 1 ומודם במחשב 2.
- אפשרי: גישה לאינטרנט.

יש מספר שיטות לוודא אם החומרה שלך נמצאת ברשימת HCL. הרשימה הבאה מפרטת כמה מהשיטות:

- בדוק את רשימת Support\Hcl.txt\ על תקליטור ההתקנה של Windows 2000 Server.
- עיין ברשימה המעודכנת ביותר של חומרה נתמכת באתר מעבדות איכות החומרה של Microsoft באתר http://www.microsoft.com/hcl/default.asp.
- אם כתובת זו אינה זמינה, גש לדף הבית של Microsoft - http://www.microsoft.com ובצע חיפוש באמצעות מילת המפתח "HCL".

דרישות תוכנה

התוכנות הבאות נדרשות להשלמת ההליכים בקורס זה:

- התקליטור המצורף לספר זה הכולל את Windows 2000 Server בגרסת Evaluation למשך 120 יום.
- מערכת הפעלה Windows 32 סיביות (Windows 9x, Windows NT 3.51, או Windows NT 4.0) על Computer2.

הוראות התקנה

הגדר את המחשב שלך בהתאם להוראות היצרן.

לתרגילים הדורשים מחשבים מרושתים, עליך לוודא שהמחשבים יכולים לתקשר אחד עם השני. Computer1 יוגדר כ-Domain Controller, ויוקצה לו חשבון מחשב בשם Server01 וה-domain יהיה microsoft.com. מחשב זה ישמש כ-Domain Controller ב-Domain ששמו microsoft.com.

ל-Computer2 יוקצה חשבון מחשב ששמו Server02 ב-Domain בשם microsoft.com. הוא ישמש כ-member server ברוב תרגילי הבריה בקורס זה.

הכנה ללימוד Windows 2000 Server

התקנת Windows 2000 Server היא חלק מערכה זו ומכוסה בפרקים 2 ו- 3. כדי להימנע מקשיים מיותרים בהשלמת תרגילים אלה, על המחשבים להכיל רק רכיבים מאושרים הנמצאים ברשימת HCL. כדאי שהמחשבים יהיו בתצורה חזקה יותר מדרישות החומרה המינימליות, ויהיו מרושתים ברשת מבודדת. המצב הרצוי הוא שלכל מחשב יהיו קיבולת זמינה של 3GB על הדיסק הקשיח וזיכרון RAM בן 128KB עבור מערכת ההפעלה ושיכלול רק תוכנות המהוות חלק מהדרכה זו. בעת עבודה עם ערכה זו, תראה התייחסות קבועה למשתנים הסביבתיים הבאים :

- %systemroot% מצביעה על תיקיה המכילה את קבצי מערכת ההפעלה של Windows 2000. ככלל %systemroot% תצביע לעבר C:\winnt.
- %windir% מצביעה לאותו מקום כמו %systemroot% ומשמשת גם ב-Windows 95 ו-Windows 98.
- %systemdrive% מצביעה לעבר השורש של מחיצת האתחול. אם התקנת את Windows 2000 ב-C:\winnt אז משתנה סביבתי זה יצביע לעבר C:.

הדרכה טכנית לאנשי מחשבים

הדרכה טכנית זמינה במיגוון דרכים, באמצעות כיתות הדרכה, הדרכה מקוונת, או לימוד בקצב-אישי באלפי אתרים ברחבי העולם.

לימוד בקצב-אישי

עבור לומדים בעלי מוטיבציה המוכנים להתמודד עם האתגר, לימוד בקצב-אישי היא השיטה הגמישה והחסכונית ביותר להגדלת הידע והכישורים. ספר זה, שהינו ספר לימוד בקצב-אישי, יכול גם לשמש כחומר עזר נלווה לקורס הנערך במרכז הדרכה.

הדרכה מקוונת

לחלופה גמישה יותר מכיתות לימוד, פנה להדרכה מקוונת. זה קרוב כמו האינטרנט ומוכן מתי שאתה מוכן. למד בקצב שלך ולפי לוח הזמנים שלך בכיתה וירטואלית, לעיתים קרובות עם גישה קלה למורה מקוון. תוכל לרכוש את המיומנות הנדרשת, ללא עזיבת שולחן העבודה. הדרכה מקוונת מכסה מגוון מוצרי Microsoft וטכנולוגיות. היא כוללת אפשרויות הנעות מ-Microsoft Official Curriculum (תוכנית הלימוד הרשמית של Microsoft) לאפשרויות שאינן זמינות בשום מקום אחר. זוהי הדרכה לפי דרישה, עם גישה למשאבי לימוד 24 שעות ביום.

http://www.click2learn.com

http://www.smartplanet.com

הערות, שאלות, רעיונות

לא נחסך כל מאמץ להבטחת הדיוק של ספר זה והתקליטור המצורף אליו. אם יש לך הערות, שאלות או רעיונות הנוגעים לספר זה או לתקליטור המצורף, אנא שלח אותם להוצאת הוד-עמי באחת השיטות הבאות:

דואר אלקטרוני:

info@hod-ami.co.il

דואר רגיל:

הוצאת הוד-עמי לספרי מחשבים בע"מ
ת.ד. 6108
הרצליה 46160

אנא שים לב שהכתובות הבאות אינן מספקות תמיכה. למידע נוסף על תמיכה בתוכנות Microsoft, בקר באתר http://www.microsoft.com/israel/support.

פרק 1

מבוא ל- Windows 2000

אודות פרק זה

פרק זה הוא מבוא למערכת הפעלה Microsoft Windows 2000. הוא מתאר את המהדורות השונות של Windows 2000 וסוקר את מבנה מערכת ההפעלה. פרק זה גם דן בתפיסה של Directory Services, ומפגיש את הקורא עם מכלול Active Directory Services, הכלול ב-Windows 2000, בגרסאות השרת השונות שלה (Server, Advanced Server, ו-Datacenter Server).

לפני שתתחיל

אין דרישות מיוחדות להבנת השיעורים בפרק זה, אף שידע בהפעלת Windows NT עשוי לסייע.

שיעור 1: סקירת Windows 2000

שיעור זה מציג את משפחת מוצרי Windows 2000, הכוללת את: Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Datacenter Serve.

השיעור מפרט את התכונות והיתרונות של Windows 2000, תוך התמקדות בתכונות הייחודיות למערכות הפעלה Windows 2000 Professional ו-Windows 2000 Server.

לאחר שיעור זה, תוכל

- לפרט את התכונות העיקריות של ארבע הגרסאות של מערכת ההפעלה Windows 2000, **ולזהות את השוני שבין המהדורות.**

זמן לימוד משוער: 15 דקות

מהדורות Windows 2000

Windows 2000 היא מערכת הפעלה רב-תכליתית הכוללת תמיכה מובנית לרשתות שרת/לקוח ורשתות Peer-to-Peer (רשתות שיוויוניות). משפחת מוצרי Windows 2000 תוכננה לאמינות גבוהה, אספקת רמות גבוהות של זמינות משאבי מערכת ואפשרות שדרוג מרשת קטנה לרשת מערכתית רחבה. Windows 2000 כוללת טכנולוגיות המפחיתות את העלות הכוללת של הבעלות (**T**otal **C**ost of **O**wnership - TCO) בכך שהיא מאפשרת לארגונים להגדיל את ערך השקעותיהם הנוכחיות בעודם מפחיתים את עלויות המחשוב הכלליות. בנוסף, Windows 2000 משלבת תמיכת אינטרנט ויישומים מקיפה, תוך שהיא נשענת על הצלחת Windows NT Server 4.0 כמערכת הפעלה פתוחה לאינטרנט המשמשת גם כשרת יישומים.

Microsoft הוציאה לאור ארבע מהדורות של Windows 2000: Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Datacenter Server.

מוצרים אלה תומכים בתשתית שרת/לקוח מתקדמת מבוססת מחשב-אישי, המפחיתה עלויות ומאפשרת התאמה מהירה של הארגון לשינויים. פלטפורמת Windows 2000 מספקת למנהלי הרשת (administrators) שליטה מוגברת על הרשתות שלהם ועל תשתיות שרת/לקוח, תוך אספקת גמישות מירבית ותמיכה בשליטה מרכזית המקובלת בדרך כלל במחשבי Mainframe/Terminal (מחשבים גדולים/מסופים).

Windows 2000 Professional

Windows 2000 Professional היא מערכת ההפעלה העיקרית של Microsoft למחשבים שולחניים עבור עסקים בכל הגדלים. זו היא מערכת הפעלה בעלת ביצועים חזקים, הכוללת אבטחה ברמת הרשת למחשבי לקוח אישיים ועסקיים. היא משלבת את

התכונות העסקיות הטובות ביותר של Windows 98, תוך שהיא נשענת על כוחה המסורתי של Windows NT Workstation. ‏Windows 2000 Professional כוללת ממשק משתמש פשוט יותר, יכולות Plug and Play, ניהול משופר של צריכת חשמל, ותמיכה במיגוון התקני חומרה. בנוסף, Windows 2000 Professional משפרת משמעותית את אפשרויות הניהול, האמינות והאבטחה של Windows NT באמצעות מערכת הצפנת הקבצים החדשה שלה וכלים לניהול יישומים.
Windows 2000 Professional תומכת במערכות בעלות מעבד בודד ועד 2 מעבדים סימטרית (Two-Way Symmetric Multiprocessing). כמו כן תומכת המערכת בקיבולת זיכרון פיסי של עד 4GB.

Windows 2000 Server

מערכת Windows 2000 Server היא שרת קבצים, הדפסות ויישומים בנוסף להיותה פלטפורמת שרת אינטרנט. היא כוללת את כל התכונות של Windows 2000 Professional בנוסף לתכונות ייעודיות-שרת חדשות רבות. ליבת Windows 2000 כוללת ערכה מושלמת של שירותים מובנים המבוססים על שירותי Active Directory. שירותי Active Directory מרכזים ניהול משתמשים, קבוצות, שירותי אבטחה ומשאבי רשת. Windows 2000 Server תומכת במערכות בעלות מעבד בודד ועד מערכות בעלות 4 מעבדים (Four-Way Symmetric Multiprocessing - SMP). כמו כן תומכת המערכת בקיבולת זיכרון פיסי של עד 4GB. היא כוללת יכולות רב-תחומיות הדרושות לקבוצות עבודה הנמצאות באתר פיזי אחד או באתרים מרוחקים בנוסף ליכולת פריסה מחלקתי של שרתי קבצים ומדפסות, שרתי יישומים, שרתי אינטרנט ושרתי תקשורת. Windows 2000 Server אידיאלית לעסקים קטנים עד בינוניים.

Windows 2000 Advanced Server

Windows 2000 Advanced Server היא מערכת הפעלה מחלקתית ושרת יישומים חזק יותר, הכוללת את כל התכונות של Windows 2000 Server בנוסף לזמינות גבוהה ויכולת שדרוג מתקדמת לפתרונות הנדרשים עבור ארגונים ומחלקות גדולות. Windows 2000 Advanced Server תומכת עד 8 מעבדים (Eight-Way SMP), משלבת Two-Way Clustering (אשכול דו-כיווני) בזמינות גבוהה והיא אידיאלית עבור עבודה אינטנסיבית בבסיסי נתונים. חומרה המבוססת על - Intel **P**hysical **A**ddress **E**xtension PAE, מאפשרת למערכת הפעלה Windows 2000 Advanced Server לנצל זיכרון פיסי רב יותר.

Windows 2000 Datacenter Server

Windows 2000 Datacenter Server היא גירסה מתמחה ברמה גבוהה של Windows 2000 Server והיא מיועדת לתת פתרונות עבור מערכות עסקיות גדולות. Windows 2000 Datacenter Server יעילה במיוחד עבור מחסני נתונים גדולים, ניתוחים כלכליים, סימולציות רחבות היקף במדעים והנדסה, עיבוד עסקאות מקוון (**O**n**L**ine **T**ransaction **P**rocessing - OLTP) ואיחוד פרוייקטים בשרת. היא גם אידיאלית כ-ISP (**I**nternet **S**ervice **P**rovider), ספק שירותי אינטרנט) בהיקף רחב ולאירוח אתרי אינטרנט. Windows 2000 Datacenter Server כוללת את ערכת התכונות

המלאה הקיימת ב- Windows 2000 Advanced Server, מספקת שירותי איזון עומסים (Load Balancing) ומשפרת שירותי Cluster (אשכול) על ידי תמיכה ב- Four-Way Clusters. המערכת היא מערכת קצה-עליון מתמחה של Windows 2000 Server התומכת ב-עד 16 מעבדים (16-Way SMP) וכן יכולה לתת תמיכה סמטרית של עד 32 מעבדים (32-Way SMP) באמצעות חומרה של יצרני ציוד מקורי (**O**riginal **E**quipment **M**anufacture - OEM).

תכונות של Windows 2000

הטבלה הבאה מפרטת את התכונות והיתרונות של Windows 2000. הטבלה מכילה נתונים הייחודיים עבור Windows 2000 Professional ו- Windows 2000 Server.

תכונה	יתרון
עלות כוללת נמוכה יותר לבעלות	• מורידה את עלות הפעלה וניהול רשת בכך שמאפשרת התקנת יישומים ושדרוג אוטומטיים, ומפשטת התקנה והגדרת מחשבי לקוח. • מפחיתה את מספר קריאות השירות בכך שמספקת ממשק Windows של Microsoft המוכר למשתמשים ולמנהלי רשת, הכולל אשפים ועזרה אינטראקטיבית. • מפחיתה את הצורך של administrators וטכנאים בנסיעות לאתרים בהם יש מחשבים לצורך שדרוג מערכת ההפעלה.
אבטחה	• מאמתת משתמשים לפני שהם מקבלים גישה למשאבים או נתונים במחשב מקומי או ברשת. • מספקת אבטחה מקומית ורשתית ומעקב אחר קבצים, תיקיות, מדפסות ומשאבים אחרים. • תומכת בפרוטוקול Kerberos ואבטחת תשתית מסוג PKI (**P**ublic **K**ey **I**nfrastructure, מפתח ציבורי).
Directory Services (שירותי ספריה)	• מאחסנת נתונים אודות משאבי הרשת, כגון חשבונות משתמשים, יישומים, משאבי הדפסה, ונתוני אבטחה. • מספקת שירותים המאפשרים למשתמשים גישה למשאבים המצויים בכל מערך רשת Windows 2000, לאתר משתמשים, מחשבים ומשאבי רשת אחרים. כמו כן מאפשרת ל-administrators לנהל ולאבטח משאבים אלה. • **Windows 2000 Server** מאחסנת ומנהלת מידע אודות שירותי Active Directory במסד הנתונים האוגר מידע על משאבי הרשת, כגון מחשבים ומדפסות. שירותי

	Active Directory מאפשרים זמינות מידע זה למשתמשים ויישומים. כמו כן הם נותנים ל-administrators שליטה על הגישה למשאבי הרשת.
ביצועים ויכולת שדרוג	• תומכת SMP על מחשבים בתצורת רבי-מיקרו-מעבדים. תומכת גם ב- Multitasking (ריבוי משימות), עיבודי מערכת ותוכנות (הכוונה היא ליכולת לפתוח מספר תוכנות שונות, כל תוכנה בחלון נפרד ובכך להריץ מספר תוכנות בו-זמנית). • **Windows 2000 Server** תומכת עד ארבעה מעבדים. מחשבים שמשמשים כשרתי Windows 2000 מיושמים בדרך כלל בתצורת שרתי קבצים והדפסות או שרתי יישומים, כגון שירותי Terminal (מסופים). • **Windows 2000 Professional** תומכת ב- עד שני מעבדים.
שירותי רשת ותקשורת	• מספקת תמיכה מובנית עבור רוב הפרוטוקולים הנפוצים של רשתות, כולל TCP/IP ו-IPX/SPX. • מספקת קישוריות לרשתות מסוג Novell NetWare, Unix ו-AppleTalk. • מספקת גישת Dial-Up (חיוג) לרשת, ובכך מאפשרת למשתמשים ניידים (שאינם נמצאים במקום קבוע) להתחבר למחשב בעל מערכת הפעלה Windows 2000. • **Windows 2000 Server** תומכת ב-256 חיבורי רשת (Sessions) של חיוג נכנס. • **Windows 2000 Professional** תומכת בחיבור בודד של חיוג נכנס לרשת. כלומר, רק אדם אחד יכול להתחבר בחיוג.
שילוב אינטרנט	• משלבת מחשבי משתמשים באינטרנט ובכך מסירה את ההפרדה בין מחשב מקומי לאינטרנט. משתמשים יכולים לדפדף ברשת, באינטראנט (Intranet) ובאינטרנט (Internet) בצורה מאובטחת לאיתור משאבים, בנוסף לשליחה וקבלה של דואר אלקטרוני והודעות. • **Windows 2000 Server** כוללת את Microsoft **I**nternet **I**nformation **S**erver (IIS), שרת מידע אינטרנט של Microsoft), שהוא פלטפורמת שרת-אינטרנט מאובטחת המשמשת לאירוח אתרי אינטראנט (Intranet) ואינטרנט (Internet) בשרתי רשת. • **Windows 2000 Professional** מספקת שרת אינטרנט אישי (**P**ersonal **W**eb **S**erver - PWS), המאפשר למשתמשים לארח אתרי אינטרנט אישיים.

תכונה	יתרון
כלי ניהול משולבים	• מספקת את האמצעים ליצירת כלים מותאמים אישית לניהול מחשבים מקומיים ומרוחקים באמצעות ממשק יחיד סטנדרטי. • מספקת אמצעים לשילוב כלי ניהול של צד-שלישי (לא של Microsoft) לתוך הממשק הסטנדרטי.
תמיכת חומרה	• תומכת ב- USB (**U**niversal **S**erial **B**us), אפיק טורי אוניברסלי, שהוא תקן עבור אפיק חיצוני המסיר מגבלות רבות שהיו קיימות באבזרי מחשב ישנים (Legacy). • תומכת בחומרת Plug and Play (הכנס-הפעל), ש- Windows 2000 מאתרת, מתקינה ומגדירה אוטומטית.

סיכום שיעור

Windows 2000 מהווה משפחה של ארבעה מוצרים: Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server ו- Windows 2000 Datacenter Server.

Windows 2000 Professional היא מערכת הפעלה עבור מחשב אישי עם תמיכה מובנת לרשתות שרת/לקוח ו- Peer-to-Peer.

Windows 2000 Server כוללת את כל התכונות של Windows 2000 Professional ותכונות חדשות נוספות ייחודיות-שרת. Windows 2000 Server מתאימה במיוחד כשרת קבצים ומדפסות או כשרת יישומים, כגון פלטפורמת שרת-אינטרנט.

Windows 2000 Advanced Server היא מערכת הפעלה חזקה יותר עבור שרת מחלקתי ויישומים הנשענת על Windows 2000 Server בכך שהיא מספקת Two-Way Clustering (אשכול דו-כיווני) ואיזון עומסים.

Windows 2000 Datacenter Server כוללת את כל התכונות של Windows 2000 Advanced Server, אך תומכת ב- Four-Way Clustering (אשכול ארבע-כיווני), ביותר מעבדים וביותר מ- 10,000 משתמשים בו-זמנית. זוהי מערכת הפעלת שרת החזקה ביותר שהוצעה אי פעם על ידי Microsoft עבור ארגונים גדולים.

שיעור 2: מבנה מערכת ההפעלה

Windows 2000 היא מערכת מבוססת-אובייקט. במילים אחרות, זו היא מערכת הפעלה מודולרית המורכבת מרכיבי תוכנה עצמאיים קטנים העובדים בשילוב ומבצעים את מטלות מערכת ההפעלה. כל רכיב כולל ערכת תפקודים (Functions) המשמשים כממשק עבור שאר המערכת.

לאחר שיעור זה, תוכל

- לזהות את הרכיבים העיקריים של מבנה מערכת הפעלה Windows 2000.
- להבדיל בין הרכיבים ב- User Mode לבין אלה שב- Kernel Mode.
- לזהות את המאפיינים של מנהלי התקנים מסוג Kernel, כולל מנהל התקן WDM (**W**indows **D**river **M**odel).

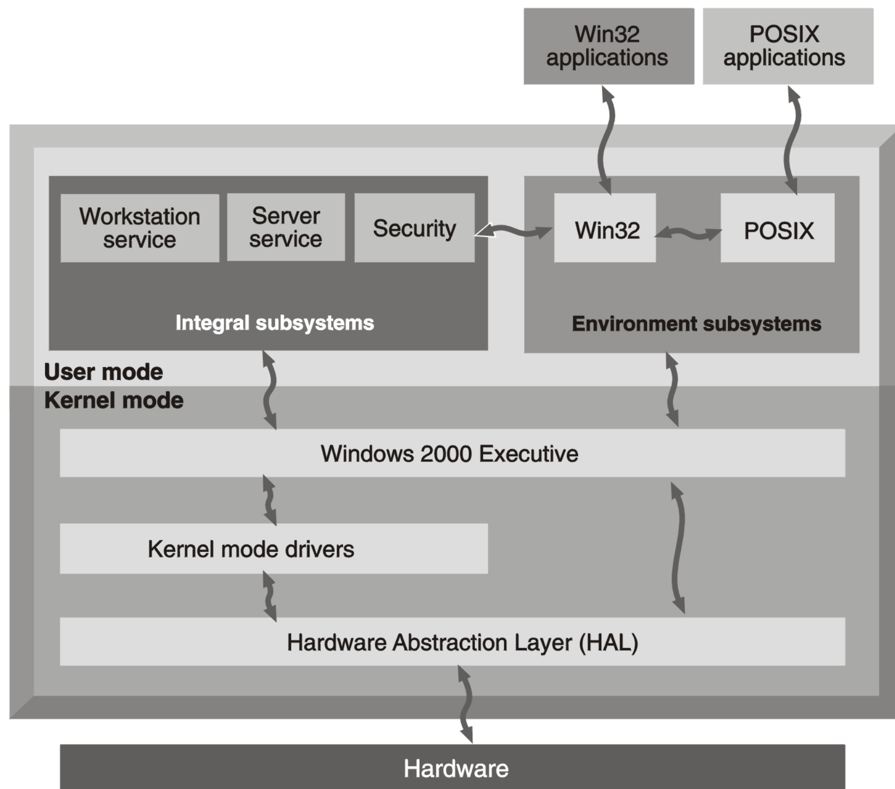
זמן לימוד משוער: 45 דקות

סקירת מבנה Windows 2000

Windows 2000 היא מערכת הפעלה ניידת, המתוכננת לעבוד על מחשבים המבוססים על CISC (**C**omplex **I**nstruction **S**et **C**omputing, מחשוב בעל ערכת פקודות מורכבת). כיון שכך, התקנים ומנהלי התקנים ניתנים להגדרה באמצעות חומרה ותוכנה. מערכת ההפעלה היא ששולטת במעבד (preemtive) ולכן יכולה להשתלט ולהפסיק כל תוכנה במהלך הפעילות. היא מתוכננת לעבוד בצורה אחידה על פלטפורמות בעלות מעבד בודד ופלטפורמות SMP, תוך שהיא מוודאת שקוד המבוצע על מעבד אחד אינו ניגש ומשנה נתונים על מעבד אחר בו-זמנית. Windows 2000 תומכת בקלט/פלט מופעל באמצעות מנות (Packet Driven I/O) הכולל דרישות מנה לשימוש חוזר (IRP) וקלט/פלט אסינכרוני, כך שיוצר בקשת קלט/פלט יכול להמשיך ולפעול, ולא להמתין לסיום ביצוע בקשת הקלט/פלט שלו. לתמיכה בתכונות השונות, Windows 2000 מתוכננת כמערכת מודולרית הבנויה ממערכת אובייקטים שניתן להפריד לשתי שכבות עיקריות: User Mode ו- Kernel Mode.

במערכות ישנות, בהן ליישומים היתה גישה ישירה למשאבים, היה מספיק שתוכנית אחת תבצע פעולה בלתי חוקית כדי שמערכת ההפעלה "תיפול" עם כל היישומים שהיא מפעילה. ב-Windows 2000, היישומים פועלים ב-User mode, שם מותאמת להם סביבה. שכבת User mode פוונה לשכבת Kernel mode ומבקשת ממנה גישה למשאבים. שכבת Kernel mode מעניקה גישה "מוגבלת" ליישומים, ולכן, כאשר יישום אחד נופל הוא "מפיל" איתו רק את חלק המשאבים שהוקצו לו ולא את כל מערכת ההפעלה. משחקי מחשב המבוססים על גישה ישירה למשאבים, ללא מתווכים כמו Kernel mode, לא יוכלו לפעול בסביבת Windows 2000 Server. תרשים 1.1 מציג סקירה כללית של מבנה מערכת ההפעלה Windows 2000. כמו כל מערכות ההפעלה,

Windows 2000 כוללת שורות קוד רבות המיועדות לספק זמינות חומרה עבור יישומים. תרשים 1.1 מציג מסגרת מושגית להבנת כיצד הקוד משתלב. עקב כך, תרשימים ממקורות שונים עלולים להיות שונים מתרשים זה.



תרשים 1.1 סקירה כללית של מבנה מערכת ההפעלה Windows 2000.

User Mode

שכבת User Mode של Windows 2000 בנויה מקבוצת רכיבים הנקראים Subsystems (תת-מערכות). תת-מערכת מעבירה דרישת I/O (פלט/קלט) ל- Kernel Mode המתאים באמצעות שירותי מערכות קלט/פלט. תת-המערכת מבודדת את המשתמשים מהצורך לדעת דבר כלשהו אודות רכיבי Kernel. שכבת User Mode מורכבת משני סוגים של תת-מערכת: תת-מערכות סביבתיות ותת-מערכות מובנות (Integral).

Environment Subsystems

תת-מערכות סביבתיות (Environment Subsystems) מאפשרות ל- Windows 2000 להפעיל יישומים שנכתבו עבור מערכות הפעלה שונות. תת-מערכות אלה מדמות מערכות הפעלה שונות על ידי הצגת ממשקי מערכות ההפעלה (API - **A**pplication **P**rogramming **I**nterfaces) שהיישום דורש שיהיו זמינים. תת-המערכות הסביבתיות מקבלות את קריאות API הנשלחות מהיישום, מסבות את קריאות API למבנה המובן למערכת Windows 2000, ומעבירות את API המוסב לרכיבים ניהוליים הפועלים ב- Kernel mode .

הטבלה להלן מסבירה את תת-המערכות ב-Windows 2000 :

תת-מערכת סביבתית	**תפקיד**
Win32	שולטת על יישומים מבוססי-Win32 ומספקת סביבה ליישומים עבור יישומי Win16 ויישומים מבוססי MS-DOS של Microsoft.
POSIX	מספקת API (ממשק מערכת הפעלה) עבור יישומים מבוססי POSIX. POSIX מתייחס לתקן ממשק מערכת הפעלה נייד שפותח ע"י IEEE (**I**nstitute of **E**lectric and **E**lectronic **E**ngineers, המכון להנדסת חשמל ואלקטרוניקה האמריקאי), להבטחת ניידות של יישומים על פני פלטפורמות שונות.

לתת-המערכות הסביבתיות וליישומים המופעלים בתוכן אין גישה ישירה לחומרה או למנהלי התקנים. הן מוגבלות לשטח כתובת מוקצה. תת-מערכות סביבתיות נאלצות להשתמש בשטחי דיסק כזיכרון וירטואלי כאשר המערכת צריכה זיכרון. בנוסף, תת-מערכות אלה פועלות בעדיפות נמוכה יותר מעיבודים ב- Kernel mode. כתוצאה מכך, יש להן פחות נגישות למחזורי יחידת העיבוד המרכזית (CPU) מאשר לעיבודים הרצים ב- Kernel mode.

הערה EMA - Microsoft **E**nterprise **M**emory **A**rchitecture, שהיא חלק ממערכות ההפעלה Windows 2000 Advanced Server ו- Windows 2000 Datacenter Server, יכולה לגרום לכמויות גדולות יותר של זיכרון RAM פיסי להיות זמינות עבור יישומים, ובכך לשפר את ביצועיהם.

Integral Subsystems

תת-מערכות אינטגרליות (Integral Subsystems) מבצעות פעולות חיוניות של מערכת ההפעלה. הטבלה הבאה מתארת כמה מתת-המערכות האינטגרליות החשובות:

תת-מערכת אינטגרלית	תפקיד
אבטחה	יוצרת אסימוני אבטחה ועוקבת אחר זכויות והרשאות המשויכים לחשבונות משתמשים. תת-המערכת מקבלת בקשות להתחברות ויוזמת אימות התחברויות. תת-מערכת האבטחה גם עוקבת איזה ממשאבי המערכת נמצאים תחת ביקורת.
שירות תחנת עבודה	תת-מערכת רשתית המספקת API לגישה לנתב הרשת. שירות תחנת העבודה מאפשר למחשב Windows 2000 לגשת לרשת (לקבל שירות).
שירות שרת	תת-מערכת רשתית אינטגרלית המספקת API כדי לאפשר גישה לשרת הרשת. שירות השרת מאפשר למחשב Windows 2000 לספק משאבי רשת (לתת שירות).

Kernel mode

לשכבת Kernel Mode במבנה Windows 2000 יש גישה לנתוני מערכת וחומרה. Kernel mode מאפשר גישה ישירה לזיכרון והוא פועל באזור זיכרון מוגן. הוא קובע מתי יופעל סדר קודים מסוים על ידי מעקב אחר קריטריונים של העדפות. לכל מטלה משויך אפיון העדפה. Kernel mode גם מקצה סדר עדיפויות לפסיקות חומרה ותוכנה, כך שחלק מקוד Kernel mode פועל ברמות גבוהות יותר של בקשות פסיקה (IRQL). Kernel mode מורכב ממספר רכיבים בעלי פעולות מוגדרות-היטב המבודדות בתוך כל רכיב: רכיב הניהול, HAL (**H**ardware **A**bstraction **L**evel, שכבת הפשטת חומרה) וערכת מנהלי התקנים של Kernel mode. שכבה זו מחליטה אם לתת ליישום גישה למשאבים, ואם כן, אז לאילו משאבים.

Windows 2000 Executive

הרכיב Windows 2000 Executive מבצע את רוב מטלות ניהול אובייקט I/O (קלט/פלט), כולל אבטחה. רכיבים שונים בתוך ה-Windows 2000 Executive, כגון VMM (**V**irtual **M**emory **M**anager, מנהל הזיכרון הווירטואלי) ומנהל הקלט/פלט, מגדירים סוג אחד או יותר של אובייקטים. רכיבים אלה מספקים שירותי מערכת ושגרות פנימיות. שירותי מערכת זמינים לתת-מערכת User Mode ולרכיבי ניהול אחרים. שגרות פנימיות זמינות רק לרכיבים אחרים בתוך ה-Windows 2000 Executive. אף רכיב אינו מורשה לגשת ישירות לשום מקרה של אובייקטים של רכיב אחר. על הרכיב

לקרוא לשגרות התמיכה המיוצאות כדי להשתמש באובייקט של רכיב אחר. כל רכיב מייצא שגרות תמיכה מסוג Kernel mode בלבד, המפעילות מופעים של סוגי אובייקט של הרכיב כאשר נקראות שגרות אלה. אם יישום ברקע של שגרת תמיכה משתנה עם הזמן, הקורא לשיגרה נשאר נייד כיון שהממשק של הרכיב המגדיר אינו משתנה.

הטבלה שלהלן מפרטת את רכיבי Kernel mode הכלולים ב-Windows 2000 Executive.

רכיב	פעולה
I/O Manager (קלט/פלט)	מספק שירותי-ליבה למנהלי התקנים (device drivers) ומתרגם פקודות קריאה וכתיבה של User mode לפקודות קריאה וכתיבה מסוג IRP. הוא מנהל את כל שאר ה-IRP העיקריים של מערכת ההפעלה. מנהל הקלט/פלט אחראי לקלט ולפלט מהתקנים ולהתקנים השונים. מנהל הקלט/פלט כולל את הרכיבים הבאים: • File Systems (מערכות קבצים) מקבלות את בקשות הקלט/פלט הייעודיות ומתרגמות אותן לקריאות ייחודיות-התקן. שרת הרשת וה-redirector (רכיב תוכנה שמקבל בקשת I/O ומחליט האם המשאב הוא מקומי, כלומר נמצא על המחשב שלנו, או שהוא נמצא ברשת) מיושמים שניהם כמנהלי התקנים של מערכת הקבצים. • Device drivers (מנהלי התקנים) הם מנהלי התקנים ברמה נמוכה המפעילים חומרה באופן ישיר לקבלת קלט או כתיבת פלט. • Cache Manager (מנהל מטמון) הוא מעין "מאגר" ביניים בזיכרון המערכת המשפר את הקלט/פלט של הדיסק על ידי אחסון קריאות מהדיסק. מנהל המטמון משפר גם את ביצועי הכתיבה על ידי הטמנת כתיבות לדיסק ברקע, ובכך מאפשר "כתיבת" נתונים גם שהדיסק עמוס בעבודה.
Security Reference Monitor (ניטור ייחוס אבטחה)	אוכף מדיניות אבטחה במחשב המקומי.
Inter**p**rocess **C**ommunication Manager (IPC, מנהל תקשורת בנוהל פנימי)	מנהל תקשורת בין לקוחות ושרתים. מנהל IPC מנהל תקשורת בין תת-מערכות סביבתיות והמנהל. תת-המערכת מתנהגת כמו לקוח הדורש מידע, והמנהל מתנהג כמו שרת המספק את הדרישה למידע. מנהל IPC כולל את שני המרכיבים הבאים: • **L**ocal **P**rocedure **C**all facility (LPC, מיתקן קריאה להליך מקומי) מנהל תקשורת כאשר לקוחות ושרתים קיימים באותו מחשב. המשאב המבוקש הוא מקומי. • **R**emote **P**rocedure **C**all facility (RPC, מיתקן קריאה להליך מרוחק) מנהל תקשורת כאשר לקוחות ושרתים קיימים במחשבים נפרדים. המשאב המבוקש נמצא ברשת.

רכיב	פעולה
Virtual **M**emory **M**anager (VMM, מנהל זיכרון וירטואלי)	מיישם ומבקר זיכרון וירטואלי, שהוא סוג ניהול זיכרון המספק טווח-כתובת פרטית עבור כל הליך ומגן על טווח-כתובת זה. VMM מאפשר למערכת ההפעלה להשתמש בשטח אחסון על הדיסק כאילו הוא חלק מהזיכרון הפיסי. זיכרון וירטואלי משתמש גם בזיכרון פיסי וגם באחסון על הדיסק. VMM גם שולט על דרישות החלפה (Paging), בכך שהוא מאפשר שימוש בשטחי דיסק כשטחי אחסון להכנסה והוצאת קוד ונתונים מ-RAM פיסי. בנוסף, ה-VMM מעביר שטחי זיכרון של יישומים שאינם בשימוש מה-RAM אל הדיסק.
Process Manager (מנהל הליכים)	יוצר ומפסיק הליכים ומטלות. הליך היא תוכנה או חלק מתוכנה, ומטלה היא ערכת פקודות ייחודית בתוך תוכנה. מנהל ההליכים מפסיק וחוזר ומתחיל מטלות, ומאחסן ושולף מידע אודות הליכים ומטלות. (ניתן לגשת אליו בעזרת Alt+Ctrl+Del).
Plug and **P**lay Manager (PnP, מנהל הכנס-הפעל)	שומר על שליטה מרכזית של הליך Plug and Play. מנהל PnP תומך בפעילות הכנס-הפעל בזמן אתחול ומשמש כממשק עם HAL, עם Windows 2000 Executive, ועם מנהלי ההתקנים. הוא שומר על שליטה מרכזית, מנתב מנהלי אפיק (Bus drivers) לביצוע ספרור והגדרה ומנתב מנהלי התקנים להוספה והפעלת התקנים. PnP Manager של Kernel mode מתאם עם הכנס-הפעל של User mode התואם לו, להשהיה או הסרה של התקנים כנדרש.
Power Manager (מנהל מתח)	שולט על מנהלי מתח API (ממשק תכנות היישום), מתאם אירועי צריכת מתח, ויוצר IRP לניהול המתח. לדוגמה, כאשר מגיעה דרישת כיבוי ממספר התקנים, מנהל המתח אוסף בקשות אלה, מוודא באיזה סדר לסדר אותן, ואז שולח IRP מתאימים לניהול המתח כנדרש.
Window Manager and **G**raphical **D**evice **I**nterface (GDI, מנהל חלון וממשק התקנים גרפיים)	מנהל את מערכת התצוגה. שני רכיבים אלה, כאשר הם מיושמים יחד כהתקן אחד בשם Win32k.sys, מבצעים את הפעולות הבאות: • **Window Manager** (מנהל חלון) שולט על תצוגת חלונות ומנהל פלט מסך. מנהל חלון אחראי גם על קבלת קלט מהתקנים כגון המקלדת והעכבר, והעברת הודעות ליישומים המקבלים קלט. • **GDI** מכיל את הפונקציות הנדרשות לציור ותפעול גרפיקה.
Object Manager (מנהל אובייקט)	יוצר, מנהל ומוחק אובייקטים המייצגים את משאבי מערכת ההפעלה, כגון הליכים, מטלות ומבנה נתונים.

HAL

HAL ‏(**H**ardware **A**bstraction **L**ayer), שכבת הפשטת/הסתרת חומרה, גורמת לכך שפרטי ממשק החומרה יהיו וירטואליים, או מוסתרים, ובכך משפרת את הניידות של Windows 2000 עבור מבני חומרה שונים. HAL מכילה קוד ייחודי-חומרה המטפל בממשקי I/O, בקרי פסיקה, ומנגנוני תקשורת של Multiprocessor (רב-מעבד). שכבה זו תוכננה במקור לאפשר ל-Windows 2000 לפעול על פלטפורמות מבוססות-Intel כמו גם על פלטפורמות אחרות כגון מערכות מבוססות Alpha, ללא צורך באחזקת שתי גרסאות נפרדות של Windows 2000 Executive.

הערה התמיכה בחומרה מבוססת-Alpha הופסקה לאחר מהדורה Windows 2000 Release Candidate One. ראה בתקליטור המצורף לספר זה בתיקיה \chapt01\articles\compaq.html.

HAL מיושמת כספריית קישורים-דינמיים ואחראית לכל תמיכה ברמת החומרה שהיא ייחודית-פלטפורמה, הדרושה לכל רכיב במערכת. HAL מייצאת שגרות תמיכה המסתירות את פרטי הפלטפורמות ייחודיות-החומרה של מטמונים, אפיקי קלט/פלט, ובקרי פסיקה. כמו כן, HAL מספקת ממשק בין רכיבי חומרת הפלטפורמה ורכיבי התוכנה של המערכת.

Kernel Mode Drivers

בדומה למערכת ההפעלה Windows 2000, מנהלי ההתקנים (device Drivers) של Kernel mode מיושמים כרכיבים מודולריים דיסקרטיים, בעלי ערכת פעולות מוגדרת-היטב. כל מנהלי ההתקנים של Kernel mode, כולל WDM ‏(**W**indows **D**river **M**odel), כוללים שגרות מנהלי התקנים סטנדרטיות מוגדרות-מערכת וכמה שגרות פנימיות, בהתאם לדרישה הייחודית של כל התקן. עבור כל שאר הרכיבים במערכת, כולל קוד User mode, חיבור להתקן מיוצג כפעולה של פתיחת קובץ אובייקט במנהל הקלט/פלט. אולם, בתוך מערכת הקלט/פלט, ההתקנים הלוגיים, הוירטואליים והפיסיים עבור כל מנהל התקן (driver) מיוצגים כאובייקטים של התקן. כל דמות טעונה של מנהל התקן (driver) מיוצגת כאובייקט מנהל התקן בתוך מנהל הקלט/פלט. מנהל קלט/פלט מגדיר את סוג האובייקט עבור אובייקטים של קבצים, אובייקטים של התקנים ואובייקטים של מנהלי התקנים (device drivers). מנהלי התקנים משתמשים באובייקטים על ידי קריאה לשגרות תמיכה של Kernel mode המיוצאות על ידי מנהל הקלט/פלט ורכיבי מערכת אחרים.

מטרות מנהלי ההתקנים של Kernel mode משותפות לרבים מיעדי התכנון של Windows 2000, כדלקמן:

- ניידות מפלטפורמה אחת לשנייה.
- יכולת הגדרה של חומרה ותוכנה.
- תמיד ניתן לעצירה או פסיקה.
- בטוח עבור ריבוי-מעבדים על פלטפורמות מרובות-מעבדים.

❖ מבוסס אובייקט.

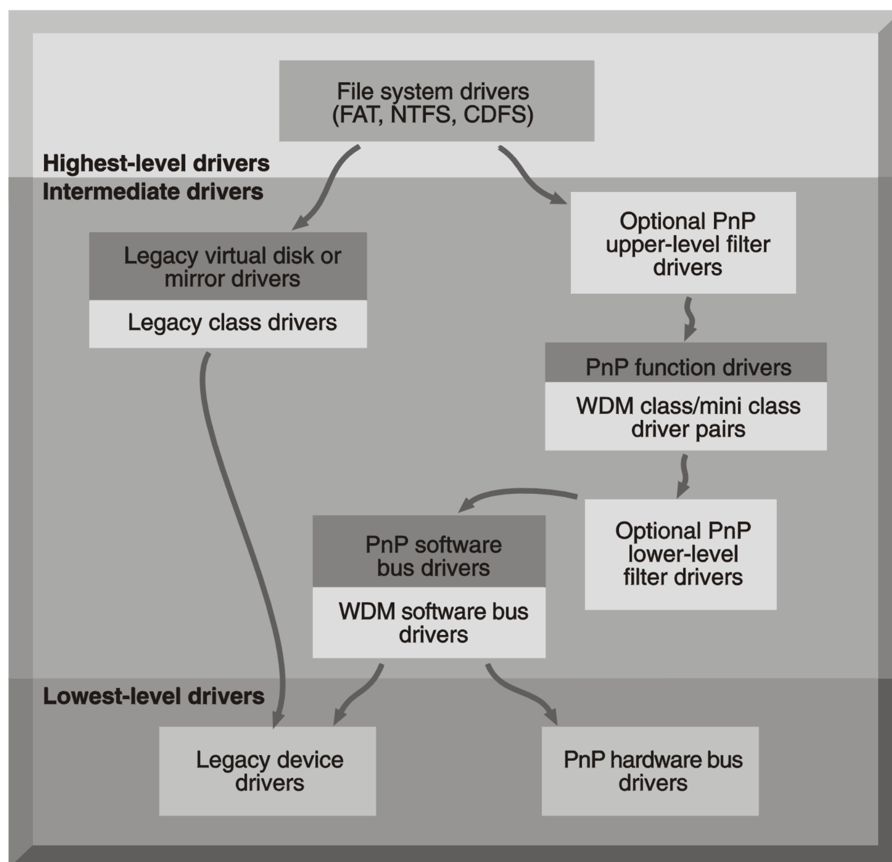
❖ קלט/פלט מופעל באמצעות מנות (Packet Driven I/O) עם IRP ניתנים למחזור.

❖ תמיכה בקלט/פלט אסינכרוני.

ישנם שלושה סוגים בסיסיים של מנהלי התקנים ב- Kernel mode:

1. מנהלי התקנים עיליים	1. Highest-level drivers
2. מנהלי התקני ביניים	2. Intermediate-level drivers
3. מנהלי התקנים בסיסיים	3. Lowest-level drivers

כמפורט בתרשים 1.2.



תרשים 1.2 שלושה סוגים של מנהלי התקנים ב- Kernel mode.

לכל אחד ממנהלי ההתקנים של Kernel mode יש מבנה שונה במקצת ותפקיד שונה לחלוטין. הטבלה הבאה מהווה סקירה של כל סוג מנהל התקן (driver). שים לב שמודל מנהל התקן Windows (WDM) הוא התקן ביניים.

סוג מנהל התקן	תיאור
Highest-Level Drivers (מנהלי התקן עיליים)	כולל FSD (**F**ile **S**ystem **D**rivers), מנהלי התקנים של מערכות קבצים), כגון מנהל התקן FAT (טבלה של הקצאת קבצים), מנהל מערכת קבצים NT (NTFS), ומנהל מערכת קבצים עבור תקליטורים (CDFS) המסופקים עם מערכת ההפעלה. מנהלי התקן עיליים תמיד נסמכים על תמיכה ממנהלי התקן ברמה נמוכה יותר. אף ש-FSD עשוי לקבל או לא לקבל תמיכה ממנהל התקן ביניים אחד או יותר, כל FSD תלוי בתמיכה מאחד או יותר מנהל התקן של ציוד היקפי.
Intermediate Drivers (מנהלי התקן ברמת ביניים)	כולל מנהלי התקנים מסוג דיסק וירטואלי, ראי, או ייחודי-לסוג-התקן. מנהלי התקן ביניים נסמכים על תמיכה ממנהלי התקן ברמה נמוכה יותר. מנהלי התקן ביניים כוללים גם את מנהלי ההתקנים הבאים: • מנהלי התקן פעולות PnP (הכנס-הפעל) השולטים על ציוד היקפי מוגדר על I/O (קלט/פלט) המבוקר על ידי מנהל התקן אפיק חומרה PnP. • מנהלי התקן מסנן PnP המתקינים את עצמם מעל או מתחת למנהלי התקן פעולות PnP במחסנית מנהלי ההתקנים עבור ציוד היקפי. • כל מנהל התקן מסווג שסופק על ידי מערכת כלשהי המייצא ממשק מוגדר-מערכת מסוג WDM Miniport/Class (סווג/קוד ייעודי מצומצם). • מנהלי התקן תוכנה באפיק הכנס-הפעל המציגים ערכת התקני-צאצאים אליהם יכולים להתחבר מנהלי התקן סינון או פעולה ברמה גבוהה יותר. • מנהלי התקן אפיק תוכנה WDM.
Lowest-Level Drivers (מנהלי התקן בסיסיים)	כולל מנהלי התקן כגון מנהלי אפיק חומרה הכנס-הפעל, השולטים על אפיק I/O, אליו מחוברים מספר התקנים היקפיים. מנהלי התקן בסיסיים אינם תלויים במנהלי התקן ברמה נמוכה יותר אלא שולטים על ציוד היקפי פיסי, כגון אפיקים. מנהלי התקנים בסיסיים כוללים גם מנהלי התקן מיושנים (Legacy) של Windows NT השולטים על ציוד היקפי פיסי באופן ישיר, כגון מנהל התקן מתאם אפיק אורח של ממשק SCSI -**S**mall **C**omputer **S**ystem **I**nterface .

WDM - Windows Driver Model

חלק ממנהלי התקן ליבה של Windows 2000 הם גם מנהלי התקן WDM (**W**indows **D**river **M**odel). מנהלי התקן WDM הם תת-קבוצה של מנהלי התקנים ברמת ביניים הנכללים בתוך מנהלי ההתקן של Kernel mode. מפרט WDM מגדיר למערכת ההפעלה את המבנה הנדרש עבור מנהלי התקנים של חומרה וממשקים. התקנים המתאימים למבנה WDM של מנהלי התקנים, נהנים מערכת שירותי קלט/פלט WDM כללית ותאימות בינארית מתוכננת בין מערכות ההפעלה Windows 98 ו- Windows 2000.

כדי להקטין את המאמץ הנדרש מספקי חומרה בתמיכה בכל הפלטפורמות המגוונות של Windows, WDM מאפשר להתקנים המיועדים ל- Windows 98 או Windows 2000 להיות מותקנים ושמישים במחשבים הפועלים בסביבת שתי מערכות הפעלה אלו.

WDM מבוסס על מבנה Class/Miniport (סיווג/קוד ייעודי מצומצם), המספק ארכיטקטורות מודולריות ניתנות להרחבה, לתמיכה בהתקנים. WDM היא טכנולוגיית ליבה עבור מחשבים מסוג SIPC - **S**imply **I**nteractive **PC**, יוזמות Zero Administration (אפס משאבי ניהול) ולתמיכת PnP החדשה במפרט USB, IEEE 1394 ויוזמת ניהול מתח מסוג OnNow Power Management.

כל סיווג (Class) WDM עושה הפשטה (Abstraction) של הנושאים המשותפים הכרוכים בשליטה על התקנים דומים. לדוגמה, נבחן מצב שבו חמישה התקנים שונים מחוברים ל- USB. אם כל מנהל התקן היה מכיל את כל הקוד הנדרש לניהול דו-שיח עם ההתקן שלו דרך אפיק USB, התוצאה היתה חמישה מנהלי התקנים (device drivers) גדולים מאוד המכילים קוד זהה בעיקרו, לטיפול בתקשורת USB. באמצעות WDM, מפתחים של מנהלי התקנים כותבים קוד Miniport (קוד ייעודי מצומצם) המנהל דו-שיח ישיר עם החומרה שלהם, וקוראים לסיווג (Class) מנהל ההתקן המתאים לביצוע רוב המשימות המשותפות. יתרון משמעותי נוסף לכתיבת Miniports (קוד ייעודי מצומצם), הוא הפחתת הסיכוי להכנסת שגיאת כתיבה (Bug) לקוד מנהל ההתקן.

WDM Layered Architecture

WDM הוא מבנה מנהל התקנים (device driver) מרובד המשתמש במנהלי התקן מסיווגים מיוחדים לאספקת תמיכה חוצה-פלטפורמות. סיווגים של מנהלי התקנים הם שכבות הפשטה (Abstraction Layers) המאפשרות למנהלי התקנים מסוג WDM לתפקד במערכות הפעלה Windows 2000 ו-Windows 98.

קיימים ארבעה סיווגים (Class) שונים של drivers:

- ❖ Miniport Drivers
- ❖ Class Drivers
- ❖ OS Services
- ❖ Virtualization Drivers

עבור כל סיווג אפיק (Bus Class) וסיווג התקן חומרה הנתמכים על ידי WDM, מספקת Windows 2000 מנהל התקן מסווג. כיון ש- Microsoft מספקת את כל תמיכת האינטגרציה עבור WDM הנדרשת בכל פלטפורמה, נדרש לכתוב רק Miniports (קוד ייעודי מצומצם) עבור כל התקני החומרה שסיווגיהם נתמכים על ידי Microsoft.

Miniport Drivers (מנהלי התקן קוד ייעודי מצומצם) – מנהלי התקן Miniport כבר מיושמים במערכת Windows 2000 בסיווגי SCSI ומתאמי רשת. במערכת Windows 2000, מושג מנהלי התקן Miniport הורחב לתמיכה ב-USB. מנהלי התקנים בעלי קוד ייעודי מצומצם הם בעלי האפיונים הבאים :

- ❖ שליטה עקיפה על חומרה באמצעות מנהל התקן אפיק ייעודי.
- ❖ תאימות קוד מקור ותאימות בינארית על פני פלטפורמות Windows.
- ❖ טעינה ופריקה דינמיות.
- ❖ תפקודיות ייעודית-חומרה בלבד.
- ❖ יכולות לחשוף (לתקשר) עם ממשקים בסיווגים רבים.

Class Drivers (מסווגים) – ההגדרה הטובה ביותר למנהל התקן מסווג הוא כמנהל התקן עבור מנהלי התקנים. מנהלי התקנים מסווגים מספקים ממשקים בין השכבות השונות של מבנה WDM. הרובד התחתון ביותר של מנהל התקן מסווג מתקשר עם ממשק הסיווג הייחודי אשר נחשף על ידי ה-Miniport (מנהל התקן בעל קוד ייעודי מצומצם). הרובד העליון של מנהלי התקן מסווגים עיליים הוא ייעודי למערכת ההפעלה. למנהלי התקן מסווגים יש גם את היכולות הבאות :

- ❖ תפקודיות ייחודית לסיווג, לא ייחודית-חומרה או ייחודית-אפיק, פרט למנהלי התקנים המסווגים כסוג אפיק.
- ❖ טעינה ופריקה דינמיות.
- ❖ תפקודיות ייחודית-סיווג בלבד (כגון ספרור).
- ❖ יכולות להציג ממשק אחיד ייחודי-סיווג לשכבות לקוחות רבים.

OS Services (מערכת הפעלה) – שכבת שירותי מערכת ההפעלה תמיד ייחודית למערכת ההפעלה. שכבה זו מפשיטה את התפקודיות הייחודית למערכת ההפעלה משכבות ה-Miniport שמתחתיה. תפקודיות זו כוללת :

- ❖ ניהול מטלות (Thread).
- ❖ ניהול ערימות (Heap).
- ❖ שירותי אירועים (Event).

Virtualization Drivers – מנהלי התקנים וירטואליים מהווים חלק ממערכות ההפעלה Windows של Microsoft החל מגירסה 3.0. הם הקבצים המוכרים כ-vxd. ב-Windows 95 וקבצי 386. בגרסאות קודמות של Windows. למנהלי התקנים וירטואליים תחת WDM יש תפקיד ייעודי. פעילותם גורמת לכך שממשקי חומרה מיושנים יהפכו וירטואליים וישלחו פקודות ייחודיות-סיווג להתקן המתאים. לדוגמה, משחק MS-DOS הפועל תחת Windows, ישתמש במנהל התקן וירטואלי כדי לעבוד עם Joystick (מוט היגוי) מבוסס USB. מנהלי התקנים אלה אינם ניגשים ישירות לחומרה,

אלא משמשים כמתווכים כך שתוכנות או חומרות מיושנות (Legacy) יוכלו לעבוד כיאות תחת הארכיטקטורה החדשה.

תמיכת מנהלי התקנים WDM עבור Windows 2000 כוללת:

- ❖ מנהל התקן מסוג Stream (זרימה), לתמיכה בזרימת נתונים ב- Kernel mode עבור לכידת וידאו, מפענח MPEG, שמע, DVD-ROM וארכיטקטורת שידור ב- Kernel mode.
- ❖ מנהל התקנים מסוג HID (**H**uman **I**nterface **D**evices, ממשקי התקנים אנושיים), לתמיכה באמצעי קלט.
- ❖ מנהלי התקנים מסווגים USB.
- ❖ מנהלי התקנים בתקן IEEE 1394.

סיכום שיעור

Windows 2000 היא מערכת הפעלה מודולרית, המורכבת מרכיבי תוכנה עצמאיים קטנים הפועלים יחד לביצוע המטלות של מערכת ההפעלה. Windows 2000 מורכבת מערכת אובייקטים הניתנים לחלוקה לשתי שכבות עיקריות: User mode ו- Kernel mode. הרכיבים העיקריים של שכבת User mode הם קבוצה של תת-מערכות המבודדות את משתמש הקצה והיישומים מהצורך לדעת דבר כלשהו על רכיבי Kernel mode. ישנם שני סוגים של תת-מערכות: סביבתי ואינטגרלי. הרכיבים העיקריים של שכבת Kernel mode הם ה-Executive, HAL, ו-kernel mode drivers. ה-Executive מבצע את רוב פעולות ניהול הקלט/פלט והאובייקטים, כולל אבטחה. HAL (שכבת הפשטת חומרה), מסתירה את פרטי ממשק החומרה ומטפלת בממשקי קלט/פלט, בקרי פסיקה ומנגנוני תקשורת מרובי-מעבדים. Kernel mode Drivers מיושמים כרכיבים מודולריים דיסקרטיים בעלי ערכה מוגדרת היטב של דרישות תפקודיות. ישנם שלושה סוגים של Kernel mode Drivers: מנהלי התקן עיליים, מנהלי התקן ברמת ביניים, ומנהלי התקן בסיסיים. מנהלי ההתקן של WDM (**W**indows **D**river **M**odel) הם תת-ערכה של מנהלי התקן מסוג Kernel mode ברמת הביניים.

מערכות ההפעלה WinNT ו- Windows 2000 הן מערכות יציבות הודות ל- user ו- Kernel. במערכות ישנות יותר, היתה ליישומים גישה ישירה למשאבים, ולכן כאשר אחת התוכנות "ביצעה פעולה בלתי חוקית" כל מערכת ההפעלה היתה נופלת. לעומת זאת, ב- Windows 2000 השיטה שונה. היישומים פועלים ב- user ושם מותאמת להן סביבה, לאחר מכן שכבת user פונה ל- kernel ומבקשת גישה למשאבים. Kernel מעניקה גישה **מוגבלת** למשאבים, לדוגמה, טווח זיכרון מסוים. לכן, כאשר אחד היישומים "נופל", הוא מפיל איתו רק את חלק המשאבים שהוקצו לו, ולא את כל מערכת ההפעלה. בדוגמה שלנו, היה נופל רק חלק מהזיכרון ולא הזיכרון כולו.

שיטה זו היא גם הסיבה לכך שמשחקים רבים לא עובדים בצורה טובה במערכות NT ו-Windows 2000: המשחקים דורשים גישה ישירה למשאבים ללא תיווך של Kernel.

שיעור 3: Windows 2000 Directory Services

Directory (ספריית הרשת) הוא אוסף מאוחסן של מידע על אובייקטים שכולם מתייחסים זה לזה בדרך כשלהי. ניתן להשוות Directory למדריך טלפון, המאחסן שמות, כתובות ומספרי טלפון של יחידים ועסקים. מדריך הטלפון הוא אוסף של אפיונים (שמות/כתובות), שבהם ניתן להשתמש כתכונות חיפוש לאיתור מידע אודות אובייקטים (מספרי טלפון) המאוחסנים במדריך. באופן דומה, **Directory Service** (שירות ספריית הרשת) מזהה משתמשים ומשאבים ברשת באופן יחידני ומספק אמצעי ארגון וגישה למשתמשים ומשאבים אלה.

לאחר שיעור זה, תוכל

- לתאר את תפקידי Directory Service
- לזהות את ההבדלים בין תחומים (Domains) לקבוצות עבודה (Workgroups).
- לתאר את שירותי ותפקיד Active Directory ולזהות את רכיביו.

זמן לימוד משוער: 45 דקות

מבוא ל- Directory Services

במערך מחשבים מבוזר או רשת מחשבים ציבורית, כמו האינטרנט, דרושים אובייקטים רבים לתמיכה במערכות, כגון משתמשים, שרתי קבצים, מדפסות, שרתי פקסים, יישומים ומסדי נתונים. המשתמשים רוצים לאתר ולנצל את האובייקטים האלה בקלות וביעילות. Administrators רוצים לנהל את אופן השימוש באובייקטים אלה. אם כל המידע הנדרש לשימוש וניהול אובייקטים אלה מאוחסן באתר מרכזי, הליך איתור וניהול המשאבים יהיה פשוט מאוד. לצרכים אלה יהיה Directory Service (שירות ספריית הרשת) שמיש ביותר.

המונחים **Directory** (ספריית הרשת) ו- **Directory Service** (שירות ספריית הרשת) מתייחסים ל- Directories המצויים ברשתות ציבוריות ופרטיות. Directory הוא מסד נתונים המורכב מאובייקטים של רשת, אליהם ניתן לגשת בדרכים שונות ורבות. הוא מאחסן מידע המתייחס למשאבי הרשת כדי לסייע באיתור וניהול משאבים אלה. Directory Service (שירות ספריית הרשת) שונה מ-Directory (ספריית הרשת) בכך שהוא מהווה גם את **מקור** נתוני ספריית הרשת וגם את **השירות** המאפשר את זמינות הנתונים למשתמשים.

Directory Service מספק את האמצעים לארגון ופישוט הגישה למשאבי מערכת מחשבים מרושתת. הוא מאפשר איתור אובייקט בהתבסס על תכונה אחת או יותר שלו. לדוגמה, Administrators עלולים שלא לדעת את שמו המדויק של אובייקט

כלשהו, אך יש להניח שידעו על אחת או יותר מתכונותיו. באמצעות Directory Services, הם יכולים לבצע שאילתה לקבלת רשימה של אובייקטים המתאימים לתכונות הידועות. למשל, הם יכולים לבצע שאילתה ב-Directory שתאתר את כל האובייקטים של מדפסות צבע המשויכים למאפייני כל הציוד שבקומה השלישית של מבנה כלשהו (או אולי שיוך מיקום שהוגדר כ"קומה שלישית").

ניתן להשתמש ב- Directory Services לביצוע מספר פעולות, כדלקמן:

- אכיפת אבטחה להגנה על אובייקטים במסד נתונים, מפולשים חיצוניים או ממשתמשים פנימיים שאינם מורשים לגשת לאובייקטים אלה.
- שכפול ה-Directory (ספריית הרשת) במחשבים אחרים ברשת, כדי שיהיה זמין למשתמשים נוספים ועמיד בפני כשל.
- חלוקת ה-Directory (ספריית הרשת) לשטחי אחסון הממוקמים במחשבים שונים על פני הרשת. בכך מתקבל יותר שטח זמין עבור ספריית הרשת כמכלול ומתאפשר אחסון מספר רב של אובייקטים.

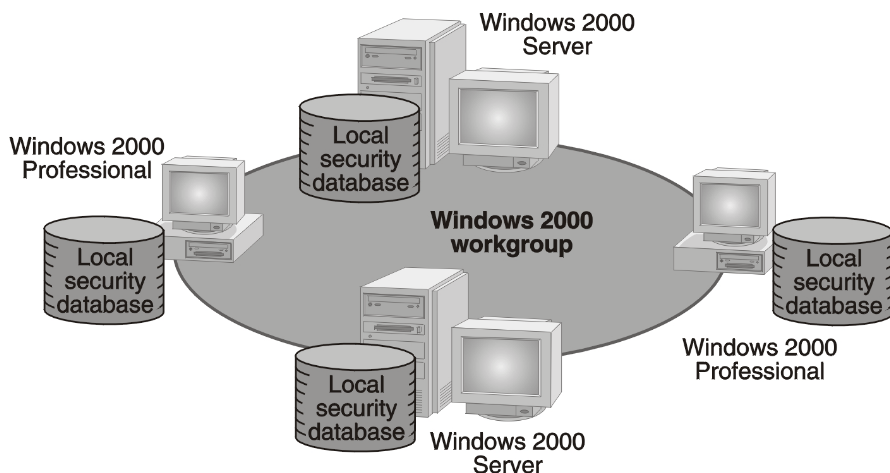
Directory (ספריית הרשת) הוא גם כלי ניהולי וגם כלי עבור משתמש הקצה. ככל שהרשת גדלה, כך גדלים המשאבים שיש לנהלם. ככל שגדל מספר האובייקטים של משאבים ברשת, כך גדל הצורך ב- Directory Service.

Workgroups and Domains

כפי שצוין קודם, Directory Service הוא אמצעי לארגון ופישוט גישה למשאבי הרשת. אולם, להקל על הגישה, Windows 2000 תומכת בשני סוגים של רשתות: קבוצות עבודה (Workgroups) ותחומים (Domains).

Windows 2000 Workgroups

Workgroup (קבוצת עבודה) היא קיבוץ לוגי של מחשבים מרושתים להם משאבים משותפים, כגון קבצים ומדפסות. **Domain** (תחום) הוא קיבוץ לוגי של מחשבים מרושתים שלהם Central Directory Database (מסד ספריית רשת מרכזי) משותף המכיל חשבונות משתמשים ונתוני אבטחה עבור התחום. לפעמים מתייחסים לקבוצת עבודה (Workgroup) כרשת שיוויונית (Peer-to-Peer), כיון שכל המחשבים בקבוצת העבודה יכולים לשתף משאבים בצורה שוויונית, ללא שרת ייעודי, כמתואר בתרשים 1.3. כל מחשב Windows 2000 Server ומחשב Windows 2000 Professional בקבוצת העבודה מחזיק **Local Security Database** (מסד נתוני אבטחה מקומי), המכיל רשימת חשבונות משתמשים ומידע אודות אבטחת משאבים עבור מחשב זה.



תרשים 1.3 Windows 2000 Workgroup.

כיון שכל מחשב בקבוצת העבודה מחזיק מסד נתוני אבטחה מקומי, ניהול חשבונות משתמשים ומשאבי אבטחה אינו מרכזי. למשתמש חייב להיות חשבון משתמש בכל מחשב שייגש אליו. כל שינוי שיעשה בחשבונות משתמשים, כמו שינוי סיסמה או הוספת חשבון חדש, חייב להיעשות בכל מחשב. אם שכחת להוסיף חשבון משתמש חדש לאחד המחשבים, המשתמש החדש לא יוכל להתחבר למחשב זה ולא יהיה לו גישה למשאבים בו.

ל- Windows 2000 Workgroups יש את היתרונות הבאים:

- ❖ קבוצת עבודה אינה דורשת מחשב הפועל תחת Windows 2000 Server להחזקת נתוני אבטחה מרכזיים.
- ❖ קל לתכנן וליישם קבוצת עבודה; אין צורך בתכנון ובניהול המורכבים הנדרשים על ידי Domain.
- ❖ קבוצת עבודה נוחה עבור מספר מחשבים מוגבל הנמצאים בסמיכות זה לזה. קבוצת עבודה הופכת לבלתי מעשית בסביבה בת יותר מעשרה מחשבים.
- ❖ קבוצת עבודה מתאימה מאוד לקבוצה קטנה של משתמשים טכניים שאינם צריכים ניהול מרכזי.

הערה בקבוצת עבודה, מחשב הפועל תחת Windows 2000 Server נקרא מחשב Stand-Alone (מחשב עצמאי).

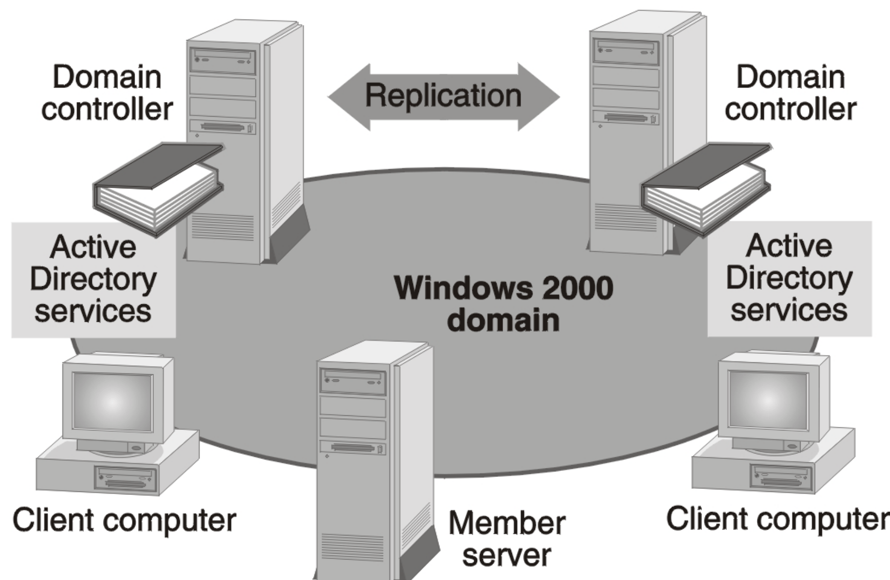
ל- Windows 2000 Workgroups יש את החסרונות הבאים:

- ❖ אין ניהול מרכזי.
- ❖ כל משתמש הוא מנהל המחשב שלו ולכן הוא חייב לעבור הכשרה כלשהיא.

Windows 2000 Domains

Windows 2000 Domain הוא קיבוץ לוגי של מחשבים מרושתים, להם Central Directory Database (מסד ספריית רשת מרכזי), המכיל חשבונות משתמשים ונתוני אבטחה עבור ה-Domain (תחום). ב- Windows 2000, מסד נתונים זה מכונה **Directory** (ספריית הרשת) והוא מהווה את מסד הנתונים שבתוך שירותי Active Directory של Windows 2000. ה-Directory (ספריית הרשת) שוכן ב-Domain (תחום) במחשבים המוגדרים כ-Domain Controllers (בקרי תחום) (תרשים 1.4).
Domain Controller (בקר תחום, ובקיצור DC) הוא שרת המנהל את נושאי האבטחה בתעבורת משתמש/תחום ומרכז את הניהול.

הערה ב-Windows NT ה-Domain Controllers הם **BDC** או **B**ackup **D**omain **C**ontrollers), בקרי תחום לגיבוי) או **PDC** (**P**rimary **D**omain **C**ontrollers), בקרי תחום ראשיים). ב-Windows 2000 יש רק סוג אחד של Domain Controller. כל בקרי התחומים (DCs) הם Peers (עמיתים, או שווים).



תרשים 1.4 Windows 2000 Domain.

Domain (תחום) אינו מתייחס למיקום בודד או לתצורת רשת ייחודית. מחשבים ב-domain יכולים להיות ממוקמים בסמיכות ברשת מקומית (LAN), או במקומות שונים בעולם, כשהם מקושרים באמצעות מערכות תקשורת שונות, כולל תקשורת אנלוגית ותקשורת דיגיטלית ISDN (**I**ntegrated **S**ervices **D**igital **N**etworks), או DSL (**D**igital **S**ubscriber **L**ines), קווי מנוי דיגיטליים). נושא התחומים נידון ביתר פירוט בסעיף הבא, "Windows 2000 Active Directory Services".

Windows 2000 Domains מספקים את היתרונות הבאים :

- Domain מספק ניהול מרכזי כיון שכל נתוני המשתמשים מרוכזים.
- Domain מספק נוהל התחברות יחיד לכל המשתמשים לקבלת גישה למשאבי רשת כגון קבצים, מדפסות, ויישומים עבורם יש להם הרשאות. משתמש יכול להתחבר למחשב אחד ולגשת למשאבים במחשב אחר ברשת, כל עוד יש למשתמש הרשאות מתאימות עבור אותו משאב.
- Domain מאפשר שדרוג כך שניתן ליצור רשתות גדולות ביותר.

Windows 2000 Active Directory Services

מכלול Active Directory Services הוא שירות ספריית הרשת הכלול ב-Windows 2000. שירותי Active Directory מספקים נקודת ניהול יחידה עבור הרשת כולה ובכך מאפשרים הוספה, הסרה ושינוי מיקום משתמשים ומשאבים בקלות.

שירותי Active Directory כוללים את ה-directory (ספריית הרשת) ובו נתונים אודות משאבי הרשת, כמו גם את כל השירותים המאפשרים זמינות ושמישות נתונים. המשאבים המאוחסנים בספריית הרשת, כגון : נתוני משתמשים, מדפסות, שרתים, מסדי נתונים, קבוצות, מחשבים ומדיניות אבטחה, נקראים אובייקטים.

תכונות Active Directory

מכלול Active Directory Services מארגן משאבים בצורה היררכית ב-Domains. **Domain** (תחום) הוא קיבוץ לוגי של שרתים ומשאבי רשת אחרים תחת שם Domain יחיד. Domain (תחום) הוא יחידת הבסיס המשמשת לשכפול (Replication) ואבטחה ברשת Windows 2000.

כל Domain כולל DC (בקר תחום) אחד או יותר. **Domain Controller** (בקר תחום, DC) הוא מחשב Windows 2000 Server המאחסן העתק מלא של Domain Directory. לפישוט הניהול, כל בקרי התחום (DCs) בשירותי Active Directory הם Peers (עמיתים), כך שניתן לבצע שינויים בכל DC (בקר תחום) והעדכונים משוכפלים בכל בקרי התחום האחרים שב-Domain תוך זמן קצר (התהליך הוא לא מיידי).

Scalability (יכולת שדרוג)

בשירותי Active Directory, ספריית הרשת (Directory) מאחסנת נתונים באמצעות **Partitions** (מחיצות), שהם חוצצים לוגיים המחלקים את ספריית הרשת לחלקים ומאפשרים אחסון אובייקטים רבים. אי לכך, ספריית הרשת יכול להתרחב ככל שהארגון גדל, ולאפשר שדרוג מהתקנה קטנה בעלת כמה מאות אובייקטים להתקנה גדולה בעלת מיליוני אובייקטים.

תמיכה בתקנים פתוחים (Open Standards Support)

שירותי Active Directory משלבים את המושג **Namespace** (טווח שמות) של האינטרנט עם Active Directory של Windows NT. השילוב מאפשר לאחד ולנהל את טווחי השמות המרובים הקיימים היום בסביבות התוכנה והחומרה ההטרוגניים ברשתות גדולות. שירותי Active Directory משתמשים ב- **D**omain **N**ame **S**ystem (DNS, מערכת הקצאת שמות תחום) ויכולים לנהל דו-שיח-נתונים עם כל יישום או ספריית רשת המשתמש ב- **L**ightweight **D**irectory **A**ccess **P**rotocol (LDAP, פרוטוקול מצומצם לגישה לספריית רשת). שירותי Active Directory גם משתפים מידע עם שירותי ספריות רשת אחרים התומכים בגרסאות 2 ו- 3 של LDAP, כגון **N**ovell **D**irectory **S**ervice (NDS, שירות ספריית הרשת של Novell).

DNS - Domain Name System

Active Directory Services משתמשים ב-DNS (**D**omain **N**ame **S**ystem) כשירות הקצאת שמות לתחומים (Domains). ולכן ה-Domain Names (שמות תחום) של Windows 2000 הם גם שמות במבנה DNS. DNS הוא שרת המחלק שמות ב-Domain. השמות הם בפורמט של שמות אינטרנט כמו www.microsoft.com. כמו כן, שרת זה מקשר בין כתובת IP של המחשב לשמו (www.microsoft.com). Windows 2000 Server משתמשת ב-DNS דינמי, שמאפשר למחשבי לקוח בעלי Dynamically Assigned Addresses (כתובות מוקצות באופן דינמי) להירשם ישירות בשרת DNS ולעדכן את טבלת השמות של DNS בצורה דינמית. DNS דינמי עשוי לבטל את הצורך של שימוש בשירותי הקצאת שמות אחרים, כגון WINS - **W**indows **I**nternet **N**aming **S**ervice שבו עשתה שימוש Windows NT.

הערה כדי ש-Active Directory Services **ותוכנות לקוח משויכות יפעלו** כנדרש, חובה **להתקין ולהגדיר שירות** DNS.

LDAP - Lightweight Directory Access Protocol

שירותי Active Directory משתמשים בתקני אינטרנט על ידי תמיכה ב-LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol). LDAP הוא תקן אינטרנט (RFC 1777) לגישה לשירותי ספריית הרשת (Directory). הוא פותח כתחליף פשוט יותר לפרוטוקול גישה X.500 (DAP). X.500 היא ערכת תקנים המגדירה שירות ספריית רשת מבוזר, שפותח על ידי ארגון התקנים הבינלאומי (ISO). שירותי Active Directory תומכים בגרסאות 2 ו- 3 של LDAP. Active Directory משתמש ב-LDAP לתעבורת נתונים בין ספריות רשת ליישומים.

הערה למידע נוסף אודות תקן RFC 1777, פנה לתקליטור המצורף לספר זה (\chapt01\articles\RFC 1777.txt).

Support for Standard Name Formats

שירותי Active Directory תומכים בכמה פורמטים נפוצים של שמות. כתוצאה מכך, משתמשים ויישומים יכולים לגשת לשירותי Active Directory על ידי שימוש בפורמט אליו הם רגילים. הטבלה הבאה מפרטת מספר פורמטים של שמות הנתמכים על ידי שירותי Active Directory.

פורמט	תיאור
RFC 822	שמות RFC 822 נכתבים בפורמט username@domainname ומוכרים לרוב המשתמשים ככתובות דואר אלקטרוני.
LDAP URLs and X.500	שמות LDAP משתמשים בשמות משויכים בפורמט X.500. URL של LDAP מציין את השרת האוחז בשירותי Active Directory ובשם המשויך של האובייקט. לדוגמה: LDAP://servername.myco.com/CN=jimsmith,OU=sys, OU=product,OU=division,O=myco,C=US.
Universal Naming Convention (UNC)	שירותי Active Directory תומכים ב-UNC המשמש ברשתות מבוססות Windows 2000 להתייחסות ל-Volumes משותפים, מדפסות וקבצים ברשת. לדוגמה: \\computer name\share name\file name \\servername.myco.com\xl\budget.xls

בכל עת, הממשק קובע את תקן השם שבו ניתן להשתמש. לעיתים ישמשו כל תקני השמות (לדוגמה, בעת התחברות), ולעיתים יידרש רק תקן מסוים (לדוגמה, תוכנית השירות LDP - כלי תמיכה של Active Directory, דורשת הקצאת שמות בשיטת LDAP).

מבנה Active Directory

שירותי Active Directory של Windows 2000 מספקים שיטה לתכנון מבנה אישי לצרכי הארגון שלך. אי לכך, עליך לבחון את המבנה העסקי והארגוני שלך לפני התקנת שירותי Active Directory. שירותי Active Directory מחלקים את הרשת לשני מבנים: לוגי ופיסי.

מבנה לוגי

בשירותי Active Directory, עליך לארגן משאבים במבנה לוגי. קיבוץ משאבים מאפשר איתור לוגי של משאב לפי שמו ולא לפי מיקומו הפיסי.

אובייקטים

Object (אובייקט) הוא ערכת אפיונים ייחודית בעלת שם המייצגת משאב רשת. **אפיון** אובייקטים (Object **Attribute**) היא תכונת אובייקטים בספריית הרשת. לדוגמה, אפיוני משתמש עשויים לכלול את שמו הפרטי ושם המשפחה, מחלקה, וכתובת דואר אלקטרוני.

בשירותי Active Directory, ניתן לארגן אובייקטים ב- **מחלקות/סיווגים** (Classes), שהן קיבוץ לוגי של אובייקטים. לדוגמה, מחלקה של אובייקטים יכולה להיות משתמשים, קבוצות, מחשבים, תחומים, או יחידות ארגוניות.

הערה Container Object (אובייקט מכולה) הוא אובייקט שיכול להכיל אובייקטים אחרים. לדוגמה, Domain (תחום) הוא אובייקט מכולה.

OU - יחידות ארגוניות

OU (Organizational unit, יחידה ארגונית) היא אובייקט מכולה, המשמש לארגון אובייקטים בתוך Domain ליצירת קבוצות ניהול לוגיות. OU יכול להכיל אובייקטים כגון חשבונות משתמשים, קבוצות, מחשבים, מדפסות, יישומים, קבצים משותפים, ויחידות ארגוניות אחרות. היררכיית היחידות הארגוניות בתוך Domain עצמאית ונפרדת ממבנה תחומים אחרים - כל Domain יכול ליצור מבנה יחידות ארגוניות עצמאי.

Domains - תחומים

יחידת הליבה של המבנה הלוגי בשירותי Active Directory היא ה-Domain (תחום). קיבוץ אובייקטים ל-Domain אחד או יותר מאפשר לשקף את ארגון החברה שלך בתוך הרשת.

כל האובייקטים של רשת קיימים בתוך Domain, וכל Domain מאחסן נתונים רק על האובייקטים שהוא מכיל. תיאורטית, Domain Controller (בקר תחום, DC) יכול להכיל עד 10 מיליון אובייקטים, אך מיליון אובייקטים ל-Domain הוא גבול התמיכה (הבדוק).

Domain (תחום) מהווה security boundary. גישה ל-Domain objects מבוקרת באמצעות **A**ccess **C**ontrol **L**ists (ACL, רשימות בקרת גישה), המכילים בתוכם **A**ccess **C**ontrol **E**ntries (ACE, ערכי בקרת גישה). מדיניות האבטחה והגדרותיה, כגון זכויות ניהול, מדיניות אבטחה ו-ACL אינם חוצים מ-Domain אחד למשנהו. ל-Domain Administrator יש זכויות מוחלטות לקביעת מדיניות אך ורק ב-Domain שלו.

הערה Domain (תחום) מכונה בשם **Partition** (מחיצה) של **שירותי** Active Directory. כל התחומים בתוך **Forest** (יער) **יוצרים** Active Directory Services (יערות מתוארים בהמשך פרק זה).

Domain (תחום) טיפוסי יכלול את סוגי המחשבים הבאים:

- **DCs הפועלים בסביבת Windows 2000 Server** – כל DC (בקר תחום) מאחסן ומתחזק העתק של ה-Directory (ספריית הרשת). פרוט בהמשך פרק זה.
- **Member Servers הפועלים בסביבת Windows 2000 Server** – member server (שרת חבר) הוא שרת שאינו מוגדר כ-DC (בקר תחום). הוא אינו

מאחסן נתוני directory ואינו יכול לאמת משתמשים ברמת ה-Domain, אלא ברמה המקומית (Local) בלבד. Member servers מספקים משאבים משותפים כגון תיקיות משותפות או מדפסות.

- **מחשבי לקוח הפועלים בסביבת Windows 2000 Professional** – מחשבי לקוח הפועלים בסביבת מחשב שולחני של משתמש ומאפשרים לו גישה למשאבים בתחום.

Trees (עצים)

Tree (עץ) הוא קיבוץ היררכי של Windows 2000 Domain(s), אחד או יותר, המאפשר שיתוף משאבים גלובלי. עץ יכול להכיל Windows 2000 Domain בודד. אולם, ניתן ליצור טווח שמות רציף גדול יותר על ידי חיבור מספר Domains (תחומים) במבנה היררכי.

כל ה-Domains (תחומים) בעץ משתפים מידע ומשאבים ומתפקדים כיחידה אחת. יש רק directory אחד בעץ תחומים, אך כל Domain אוחז את חלק ה-Directory המכיל את נתוני חשבונות המשתמשים של תחומו הוא. בתוך עץ, משתמש המתחבר דרך Domain (תחום) אחד יכול להשתמש במשאבים בתחום אחר, כל עוד יש למשתמש את ההרשאות הנדרשות.

Windows 2000 משלבת את נתוני ה-Directory (ספריית הרשת) של כל התחומים לספרייה אחת בודדת, ובכך מאפשרת נגישות גלובלית לנתוני כל Domain (תחום). בנוסף, כל Domain מספק אוטומטית תת-ערכה של נתוני התחום שלו לשירותי Active Directory כאינדקס, הנמצא על ה-Domain Controllers (בקרי התחומים). משתמשים מחפשים באינדקס זה משתמשים אחרים, מחשבים, משאבים ויישומים בכל עץ התחומים. לכל התחומים בעץ בודד יש **schema** (סכמה) משותפת, שהיא הגדרה רשמית של כל סוגי האובייקטים שניתן לאחסן בפריסת Active Directory. בנוסף, לכל התחומים בעץ בודד יש **global catalog** (קטלוג גלובלי), שהוא מחסן הנתונים המרכזי עבור אובייקטים בעץ (Tree) או יער (Forest).

לכל ה-Domains בתוך עץ (Tree) בודד יש גם טווח שמות משותף ומבנה שמות היררכי. **Namespace** (טווח שמות) היא ערכת חוקים לנתינת שמות המספקת את המבנה ההיררכי או Path (נתיב), של עץ. בהתאם לתקני DNS קובעים כי Domain name של Child-Domain (תחום-צאצא) הוא השם היחסי של שם הצאצא עם סיומת שהיא שם תחום ההורה. שם של עץ תחומים צריך להוביל לשם החברה כפי שהוא רשום באינטרנט.

האתר של חברת Microsoft הוא Domain ראשי. כתובת ה-Domain היא microsoft.com. אם החברה תפתח Child-domain חדש בשם Shalom, אז כתובתו תהיה shalom.microsoft.com. ה-Domain החדש (shalom) יורש את שם ה-Parent-domain.

בשירותי Active Directory, עץ (Tree) מוגדר על ידי:

- ❖ היררכיה של Domains (תחומים).
- ❖ טווח שמות רציף (Namespace).
- ❖ יחסי אמון בין תחומים, מבוססי פרוטוקול Kerberos.
- ❖ סכמה (Schema) משותפת.
- ❖ קטלוג גלובלי (Global Catalog) של רשימת כל האובייקטים בעץ.

יערות (Forests)

forest (יער) הוא קיבוץ של עץ (Tree) אחד או יותר. יערות מאפשרים לארגונים לקבץ מחלקות (או לאפשר לשני ארגונים לשלב בין רשתותיהם) שאינן משתמשות באותה צורה של נתינת שמות ופועלות בנפרד, אך נדרשות לתקשר עם הארגון כולו.

העצים ביער שותפים לאותה **Schema** (סכמה) ואותם חוקים הנוגעים לעבודתם המשותפת של אובייקטים. לכל ה-Domains ביער יש **Global Catalog** (קטלוג) ומכולת (Container) תצורה משותפת.

יער מוגדר על ידי:

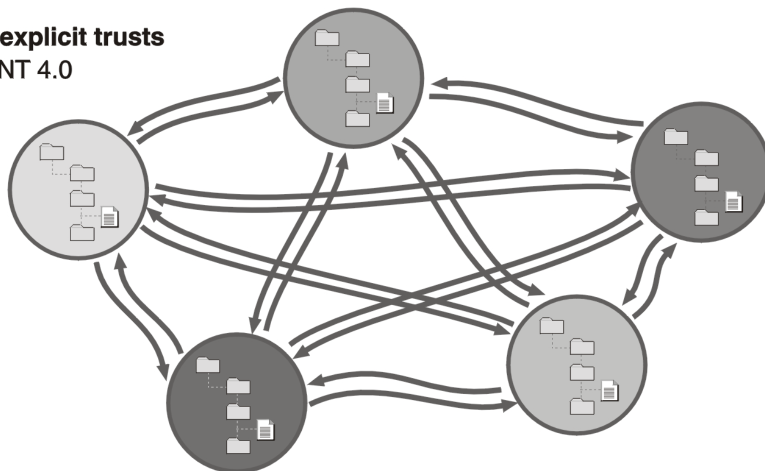
- ❖ סדרת עצים אחת או יותר.
- ❖ טווחי שמות לא-מחוברים בין עצים אלה.
- ❖ יחסי אמון בין עצים, מבוססי פרוטוקול Kerberos.
- ❖ סכמה משותפת.
- ❖ קטלוג גלובלי של רשימת כל האובייקטים ביער.

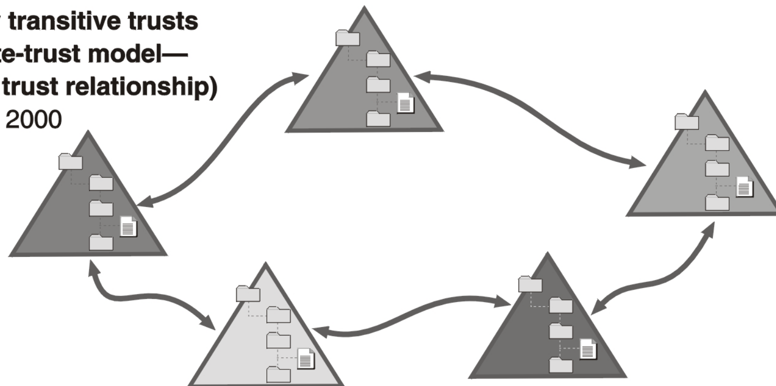
האובייקטים של ה-Domain Trees, המהווים את היער, זמינים לכל האובייקטים של המשתמשים ביער. אולם, בעת גישה לאובייקטים באותו יער אך בעצים שונים, על המשתמש לדעת את מלוא שם ה-Domain או לפחות להיות מסוגל לעיין (Browse) ולזהות הררכיית תחומים בעת דפדוף ברשת הארגון הפנימית בעת חיפוש אחר משאבים.

Trust Relationships (יחסי אמון)

תחומים (Domains) בעץ מחוברים יחד בצורה שקופה על ידי יחסי אמון דו-כיווניים מבוססי פרוטוקול Kerberos. **יחסי אמון דו-כיווניים מבוססי פרוטוקול Kerberos** (Kerberos transitive trust), משמעותם היא שאם Domain A סומך על Domain B, ו-Domain B סומך על Domain C, הרי ש-Domain A סומך על Domain C. אי לכך, ל-Domain המתחבר לעץ יש מייד יחסי אמון עם כל תחום בעץ. יחסי אמון אלה יוצרים מצב בו כל האובייקטים בכל התחומים זמינים לכל שאר התחומים בעץ.

יחס אמון (Trust relationship) הוא קשר בין לפחות שני Domains (תחומים) שבו ה-Trusting domain מכבד את אימות ההתחברות של ה-trusted domain. ניתן להעניק לחשבונות משתמשים וקבוצות שהוגדרו ב-Trusted domain זכויות והרשאות משאבים ב-Trusting domain, אף שחשבונות אלה אינם קיימים במסד נתוני ספריית הרשת (Directory Database Services) של ה-Trusting domain. תרשים 1.6 מתאר את ההבדל בין סמיכות דו-כיוונית של Windows NT והדגם הפשוט יותר של סמיכויות דו-כיווניות משורשרות (Two-way Transitive Trusts) ב-Windows 2000.





תרשים 1.6 יחסי אמון Windows NT Domains **וב-** Windows 2000 Domains.

ב-Windows NT ובגרסאות קודמות, יחסי אמון בין-תחומים מוגדרים באמצעות One-Way Trusted Accounts (יחסי אמון חד-כיווניים) בין DCs (בקרי תחום). כל מערכת יחסי אמון חייבת להיווסד ולהיות מנוהלת באופן עצמאי. ניהול יחסי אמון חד-כיווניים בין Domains (תחומים) על פני רשת גדולה היא משימה מורכבת.

Windows 2000 Trust Relationship – כאשר Domain (תחום) מתחבר ל- Windows 2000 domain Tree, מתהווים יחסי האמון, בין התחום החדש לתחום השורש או תחום ההורה של העץ, באופן אוטומטי. Transitive Trust היא תכונה של מערכת Kerberos, המספקת את האימות וההרשאה המבוזרים במחשבי Windows 2000.

Two-way Trust Relationship – מנהל הרשת יכול להגדיר חשבונות יחסי אמון חד-כיווניים עבור תחומים מסוימים, כאשר יחסי אמון דו-כיווניים אינם מתאימים. יכולת זו קיימת לצורך תמיכה בחיבור ל-Windows NT 4.0 ותחומים מוקדמים יותר, ומאפשרת הגדרת יחסי אמון עם תחומים ביערות אחרים.

הערה ניתן להגדיר יחסי אמון חד-כיווניים כנדרש באמצעות תכונות התחום ב-Snap-In (תוסף תוכנה) של ה-Site Manager (מנהל האתר). **Snap-in** (תוסף תוכנה) הוא סוג של כלי (תוכנה קטנה/שגרת פקודות) הניתן להוסיף ל- Console הנתמך על ידי MMC (**M**icrosoft **M**anagement **C**onsole). MMC ו-Snap-ins נידונים בפירוט בפרק 6.

שימו לב! ב-Windows NT 4 אין אפשרות של שירשור יחסי אמון בין Domains.

מבנה פיסי

המבנה הפיסי של שירותי Active Directory משפיע על יעילות השכפול בין Domain Controllers (בקרי תחום).

Domain Controllers

DC (בקר תחום) הוא מחשב Windows 2000 Server המאחסן העתק של ה-Directory (ספריית הרשת). לכל ה- DCs שב-Domain יש העתק מושלם של ה-directory. כאשר מתבצעת פעולה שתוצאותיה עדכון ה-directory (ספריית הרשת), Windows 2000 משכפלת את העדכון באופן אוטומטי בכל שאר ה-DCs שב-Domain. עדכונים חשובים במיוחד, כגון שינוי סיסמה או נעילת חשבון לקוח, משוכפלים מייד בכל ה-Domain. עדכונים חשובים פחות מחכים לעדכון המתבצע כל מספר דקות, אלא אם כן מתבצע עדכון/שכפול ידני.

אתה יוצר חשבון משתמש פעם אחת, הנרשם על ידי Windows 2000 ב-Directory אשר ב-Domain. כאשר משתמש מתחבר למחשב שב-Domain, בקר תחום בודק את ה-directory (ספריית הרשת) לאיתור שמו של המשתמש, סיסמה והגבלות התחברות, כדי לאמת אותו (את המשתמש). כאשר יש מספר Domain Controllers, הם משכפלים את נתוני ה-directory של עצמם תקופתית. רק מחשבים הפועלים תחת מערכות הפעלה Windows 2000 Server, Advanced Server, או Datacenter Server יכולים להיות מוגדרים כ- Domain Controllers (בקרי תחום) ברשת מבוססת Windows 2000.

Sites (אתרים)

המושג **Site** (אתר) מוכר מיישומי משפחת מוצרי Microsoft BackOffice. מושג זה נכלל ביישומים של שירותי Active Directory; אולם, הוא שונה ממושג האתר שבמוצרי Microsoft BackOffice, כגון Microsoft Exchange. בשירותי Active Directory של Windows 2000, מושג האתר משתמש במושג הקיים **I**nternet **P**rotocol (IP) Subnets (תת-רשתות בפרוטוקול אינטרנט) לקביעת גבולות אתרים משקולי Replication Traffic (תעבורת שכפול). ההבדל הבסיסי בין אתרים בשירותי Active Directory ומוצרי BackOffice השונים הוא שאתרי Active Directory מוגדרים כטווח IP Subnets (תת-רשת IP). במוצרי BackOffice כגון Microsoft Exchange Server, אתר הוא קיבוץ לוגי של שרתים שניתן להגדיר בלי להתייחס למיקומם הפיסי של השרתים עצמם.

ביסודו, Active Directory הוא אוסף של טווחי תת-רשתות IP. לדוגמה, אתר יכול להיות מוגדר כטווח Subnet (תת-רשת) 192.168.10.0/24 עד 192.168.20.0/24. אתר אחר, בקצהו השני של קישור WAN יכול להיות 172.20.10.0/24 עד 172.20.20.0/24. אולם, שני האתרים עשויים להיות חלק מאותו Windows 2000 Domain.

הערה כיתוב 24/ שמשמש בדוגמה הקודמת, מייצג 24 סיביות "1" משמאל לימין בכתובת המיסוק (Subnet Mask) אשר בייצוג עשרוני תיראה כך 255.255.255.0. כיתוב 22/ מייצג 22 סיביות "1" משמאל לימין בכתובת המיסוק, ולכן בייצוג עשרוני תיראה כך 255.255.252.0.

אחד היתרונות של שירותי Active Directory הוא ש-Domains יכולים לגשר על מרחקים גיאוגרפיים בטופולוגיות שונות המחוברים בקישורי WAN, ועדיין להישאר שקופים למשתמש. אולם, מידת רוחב פס WAN הזמין היא תמיד שיקול. על ידי הגדרת קבוצות תת-רשת מקומיות כאתרים, מנהלי רשת יכולים לשלוט על Replication Traffic (תעבורת השכפול) שבין תת-רשתות, ועקב כך בין אתרים. התוצאה היא תעבורת שכפול מופחתת על פני קישורי WAN.

רעיון האתר משמש גם עבור משתמש המחפש DC (בקר תחום) כדי לקבל אישורי התחברות. משתמש מאתר אחד עשוי לשבת מול תחנת עבודה באתר אחר. כדי שהמשתמש יאושר, ייתכן שיהיה צורך למצוא בקר תחום באתר המשתמש. השוואת אתר המשתמש לאתר תחנת העבודה (דהיינו השוואת תת-רשתות) יסייע באיתור DC מתאים.

סיכום שיעור

שירות Active Directory מספק את האמצעים לארגון ופישוט גישה למשאבים במערכת מחשב מרושתת. Windows 2000 תומכת בסביבות רשת מאובטחות בהן משתמשים יכולים לשתף משאבים משותפים, ללא תלות בגודל הרשת. Windows 2000 תומכת בשני סוגים של רשתות: Workgroups (קבוצות עבודה) ו-Domains (תחומים). Windows 2000 כוללת שירותי Active Directory, שהוא שירות ספריית רשת המספק נקודת ניהול אחת עבור הרשת כולה. שירותי Active Directory מאפשרים להוסיף, להסיר, ולהזיז משתמשים ומשאבים במהירות. היא מפרידה לחלוטין את המבנה הלוגי של היררכיית ה-Domain מהמבנה הפיסי. המבנה הלוגי מורכב מאובייקטים, יחידות ארגוניות (OU), Domains (תחומים), עצים (Trees) ויערות (Forests). כאשר מחברים Domain ל-Windows 2000 domain tree, נוצרים Trust relationship מבוססי פרוטוקול Kerberos באופן אוטומטי בין ה-Domain החדש ל-Root domain או Parent domain של העץ. המבנה הפיסי של היררכיית ה-Domain מורכב מ-DCs ו-Sites.

שאלות סיכום

השאלות הבאות מיועדות לחיזוק הנושאים העיקריים שנידונו בפרק זה. אם אינך יודע את התשובה לשאלה, חזור ועיין בשיעורים המתאימים ונסה לענות על השאלה שנית. תשובות לשאלות נמצאות בנספח A. השאלות מופיעות באנגלית ואח"כ בעברית.

The following questions are intended to reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A.

1. A client has asked you to recommend the appropriate server edition(s) of Windows 2000 for his environment. Your recommendation is based on the following characteristics:

   - All remote offices are connected to the corporate headquarters and data center by high- speed (greater than 10 Mbps) connections.
   - All 10,000 users run Windows 2000 Professional or Windows 98.

   And the following functional requirements:

   - All sites will access a high- availability server cluster running a Microsoft SQL Server 7.0 database. A two- server cluster with six processors per computer is adequate, and there are no plans to upgrade the cluster.
   - All other servers will run an edition of Windows 2000 to provide Active Directory services, basic file and print services, and dial- in access to the network.
   - These servers will run anywhere from one to four processors.
   - Processor sizing will be based on the number of users supported at each site. For example, a small remote site will contain a single processor server while all servers in the corporate site will contain four processors. For simplicity, one server edition of Windows 2000 will be selected for all computers serving this role.
   - Each domain in Active Directory services will support 2500 users.
2. Why is a WDM driver preferred over legacy Windows NT drivers?
3. How does Windows 2000 protect Executive services from user mode applications?
4. What component of the Executive makes Windows 2000 preemptible?
5. What is the primary difference between a workgroup and a domain?
6. What is the structure and purpose of a directory service?

1. לקוח ביקש ממך להמליץ על גרסת שרת Windows 2000 המתאימה לסביבת העבודה שלו. המלצתך מבוססת על האפיונים הבאים:

❖ כל המשרדים המרוחקים מחוברים למשרד הראשי ולמרכז המידע באמצעות חיבורים מהירים (מהירות גדולה מ- 10Mbps).

❖ כל 10,000 המשתמשים מפעילים מערכות הפעלה Windows 2000 או Windows 98.

כמו כן קיימות הדרישות התפקודיות הבאות:

❖ כל האתרים יגשו לאשכול שרתים מסוג זמינות גבוהה המריץ Microsoft SQL Server 7.0 Database. בארגון קיים אשכול בעל שני שרתים כשבכל מחשב ששה מעבדים, ואין כוונות לשדרג את האשכול.

❖ כל שאר השרתים יפעלו תחת מערכות הפעלה Windows 2000 לאפשר ולספק שירותי Active Directory, שירותי קבצים ומדפסות בסיסיים וגישה לרשת באמצעות חיוג.

❖ שרתים אלה יהיו בעלי אחד עד ארבעה מעבדים כל אחד. מספר המעבדים יתבסס על מספר המשתמשים שכל אתר תומך. לדוגמה, אתר מרוחק קטן יכיל שרת בעל מעבד בודד בעוד שכל השרתים באתר המשרד הראשי יכילו ארבעה מעבדים. למען הפשטות, תיבחר גרסת שרת של Windows 2000 עבור כל המחשבים המשמשים בתפקיד זה.

❖ כל Domain בשירותי Active Directory יתמוך ב- 2,500 משתמשים.

2. מדוע עדיף להשתמש במנהל התקנים מסוג WDM על פני מנהל התקנים מסוג ירושה של Windows NT?

3. כיצד Windows 2000 מגנה על שירותי Executive מיישומי מצב משתמש?

4. איזה רכיב ב-Executive מאפשר מערכת ריבוי משימות מאולצת (preemptiv) ב-Windows 2000?

5. מה ההבדל העיקרי בין Workgroups (קבוצת עבודה) ל-Domain (תחום)?

6. מהו המבנה של Directory Services ומהי מטרתו?

פרק 2

התקנה והגדרה של Windows 2000 Server

אודות פרק זה

פרק זה הוא הכנה להתקנת Windows 2000 Server. הוא סוקר את המידע הדרוש להכנת ההתקנה ואת הצעדים המקדימים להתקנה. הפרק מתקדם דרך שלבי ההתקנה השונים וממשיך ודן בשדרוג ל-Windows 2000 Server. הפרק מסתיים בשיעור על איתור תקלות התקנה של Windows 2000 Server.

לפני שתתחיל

לביצוע השיעורים בפרק זה נדרש הציוד הבא:

- מחשב הממלא אחר דרישות סף של חומרה כמפורט בהקדמה.
- תקליטור התקנה של Windows 2000 Server.

שיעור 1: הכנות להתקנת Windows 2000 Server

לפני התקנת Windows 2000 Server, עליך לאסוף מידע ולקבל החלטות על אופן התקנת התוכנה. פרק זה מספק את היסודות הנדרשים להתקנת Windows 2000 Server. הוא מתאר את המטלות שעליך להשלים לפני ביצוע ההתקנה עצמה.

לאחר שיעור זה, תוכל

- להכין התקנה של Windows 2000 Server על ידי השלמת מטלות מקדימות להתקנה כגון זיהוי דרישות חומרה ואיסוף המידע הדרוש לביצוע ההתקנה.

זמן לימוד משוער: 90 דקות

הכנות להתקנה

בעת ההתקנה, מבקשת תוכנית ההתקנה של Windows 2000 מידע על אופן ההתקנה והתצורה הנדרשת של Windows 2000. עליך לאסוף את כל המידע הנדרש. הכנה טובה מונעת תקלות בעת ההתקנה ואחריה.

לפני התחלת הליך ההתקנה של Windows 2000, עיין ברשימת המטלות המפורטות בטבלה להלן. כל מטלה נידונה ביתר פירוט בסעיפים הבאים. תחילה יש להשלים רק את שתי המטלות הראשונות בפרק זה - תוך שהנך מוודא שהמחשב שברשותך עומד בדרישות הסף של החומרה ולאחר ביצוע בדיקת תאימות החומרה. שאר המטלות מושלמות בעת ההתקנה הממשית של Windows 2000 Server, המתבצעת בתרגילים המופיעים בהמשך פרק זה. טבלה זו מיועדת רק להכינך להתקנה, כך שתוכל להתקין את Windows 2000 Server ללא עיכובים מיותרים.

מטלות	
❐	ודא שהמחשב שלך עומד בדרישות הסף של החומרה. לדוגמה, מעבד Pentium 133Mhz לפחות, אם כי רצוי מעבד חזק הרבה יותר.
❐	בדוק את כל החומרה (מתאמי רשת, מנהלי התקני התצוגה, כרטיסי קול, כונני תקליטורים, כרטיסי לוח-אם וכו') ודא שהיא תואמת על ידי עיון ב- HCL (**H**ardware **C**ompatibility **L**ist), רשימת חומרה תואמת עבור Windows 2000).
❐	קבע את האופן שברצונך לחלק למחיצות את הדיסק הקשיח עליו תתקין את Windows 2000 Server. בחר מערכת קבצים המתאימה לדרישותיך המספקת את השירותים הדרושים. בחר NTFS, אלא אם נדרש להפעיל יותר ממערכת הפעלה אחת מהמחשב.

מטלות (המשך)	
❒	בחר בסוג רשיון הפעלה. תוכל להחליף לרשיון מבוסס לקוח (Per-Seat) מרשיון מבוסס שרת (Per-Server), אך לא להיפך.
❒	בחר את סוג הרשת (Workgroups או Domain) אליו יצטרף המחשב שלך. אם ההתחברות היא ל-Domain (תחום), נדרש מידע נוסף כגון שם Domain ושם חשבון המחשב שנוצר עבורך. כשברשותך חשבון Administrator וסיסמה עבור ה-Domain (תחום), תוכל ליצור חשבון למחשב בתוך ה-Domain.
❒	קבע אם לבצע התקנה חדשה או לשדרג גירסה קיימת של שרת NT. לא ניתן לשדרג Windows NT Workstation או Windows 9x ל-Windows 2000 Server.
❒	בחר מהיכן תתבצע ההתקנה: דיסקטים, תקליטור או דרך הרשת.
❒	בחר את הרכיבים שנדרש להתקין, כגון Networking Services או Microsoft Indexing Service.

בנוסף למטלות המפורטות ברשימה לעיל, יש לבצע את המטלות הבאות להכנת ההתקנה ומניעת תקלות אפשריות.

עבודה עם DNS -

בעת יצירת Windows 2000 Domain, חייב שירות DNS (**D**omain **N**ame **S**ystem) להיות מוגדר ופעיל. אם נדרש להצטרף ל-Domain (תחום), יש לדעת את שם DNS שהמחשב מצטרף אליו. אם DNS אינו פעיל, ניתן להתקין אותו בעת יצירת DC (בקר תחום) או בעת קידום שרת לתפקיד DC.

רישום נתונים

עליך לרשום את הנתונים הבאים: מערכת הפעלה קודמת (אם היתה), שם המחשב (אם המחשב ברשת), שם קבוצת העבודה (Workgroup) או ה-Domain (אם המחשב ברשת), וכתובת IP (אם אין שרת DHCP - **D**ynamic **H**ost **C**onfiguration **P**rotocol, או אם שרת DHCP הקיים לא ישמש למיעון IP דינמי).

הערה DHCP - הינו שרת המחלק, באופן אוטומטי, כתובות IP.

גיבוי קבצים

לפני התקנת Windows 2000 Server, גבה את הקבצים שברצונך לשמור. ניתן לגבות לדיסק, קלטת גיבוי, או למחשב אחר ברשת.

ביטול דחיסה

לפני התקנת Windows 2000 יש לבטל דחיסה ב-Volumes שנדחסו באמצעות DriveSpace או DoubleSpace. אין להתקין Windows 2000 על כונן דחוס, אלא אם נדחס באמצעות תוכנית שירות דחיסה של NTFS. Volumes של DriveSpace או DoubleSpace נוצרות ב-Windows 9x. לא ניתן לשדרג מערכת הפעלה Windows 9x ל-Windows 2000 Server אך היא יכולה להמשיך ולפעול בדו-קיום על מחשב הפועל בסביבת Windows 2000 Server.

ביטול שיקוף דיסק (Disk Mirroring)

אם אתה מתקין עותק נקי (חדש) של Windows 2000 ובמחשב היעד הותקן Windows NT Disk Mirroring (שיקוף דיסק Windows NT במובן של יצירת **תמונת ראי**. כלומר, שני הדיסקים רושמים נתונים במקביל, כך שאם דיסק אחד מפסיק לתפקד, ניתן להמשיך ולעבוד עם הדיסק השני), בטל (Break) אותו לפני הפעלת תוכנית ההתקנה. תמיד ניתן לחזור ולהגדיר שיקוף דיסק לאחר השלמת ההתקנה. אם אתה משדרג מערכת ל-Windows 2000, תוכל להשאיר את שיקוף Windows NT, בעת הפעלת תוכנית ההתקנה.

הערה להשלמת התקנה חדשה של Windows 2000 לא נדרש לבטל שיקוף דיסק ברמת החומרה, כיון שמערכת ההפעלה אינה מודעת ל-RAID (**R**edundant **A**rray of **I**nexpensive **D**isks) המיושם בחומרה.

ניתוק התקני אל-פסק (UPS)

UPS - התקן עם סוללה הנמצא בין החשמל שבקיר למחשב. בעת הפסקת חשמל ו/או נפילת מתח, הסוללה שבהתקן מספקת חשמל למחשב, ובכך מאפשרת את כיבוי השרת באופן מסודר.

אם התקן אל-פסק כלשהו מחובר למחשב היעד שלך, נתק את הכבל הטורי, בין ה-UPS למחשב, לפני הפעלת תוכנית ההתקנה. תוכנית ההתקנה של Windows 2000 מנסה לאתר התקנים המחוברים ליציאות הטוריות באופן אוטומטי, וציוד אל-פסק עלול ליצור תקלות בהליך האיתור.

כאשר Windows 2000 מזהה חומרה, היא שולחת אות חשמלי לכל היציאות ובהתאם לתגובה קובעת את סוג ההתקן. אם הכבל הטורי של ה-UPS מחובר, ייווצר קצר.

הערה הכבל הטורי בין ה-UPS למחשב מיועד להעביר אות חשמלי כאשר יש נפילת מתח. אז השרת בתגובה נכנס לפעילות Shutdown. לא תמיד כבל זה מחובר.

סקירת יישומים

לפני הפעלת תוכנית ההתקנה Windows 2000 Server Setup Program, קרא את קובץ Readme.doc (בספריית השורש של תקליטור ההתקנה של Windows 2000 Server), למידע אודות יישומים שיש למנוע פעילותם או להסירם לפני הפעלת תוכנית ההתקנה. ייתכן שתצטרך להסיר תוכניות איתור וירוסים, שירות רשת של צד-שלישי, או תוכנות לקוח לפני הפעלת Windows 2000 Server Installation. יש מחשבים בהם צריך לבטל את האנטי-וירוס דרך ה-BIOS.

בדיקת סקטור האתחול לאיתור וירוסים

וירוס בסקטור האתחול (Boot Sector) יגרום לכשל התקנת Windows 2000. כדי לוודא שסקטור האתחול אינו נגוע בווירוס כלשהו, הפעל את קובץ Makedisk.bat בספריית \Valueadd\3rdparty\CA_antiv שבתקליטור ההתקנה של Windows 2000 Server. תוכנית השירות Makedisk.bat יוצרת דיסקט המשמש לבדיקת סקטור האתחול. לאחר יצירת דיסקט זה, אתחל את המחשב כאשר הדיסקט בכונן. פעולה זו תפעיל תוכנית בדיקת וירוסים על סקטור האתחול. לאחר סיום הפעלת תוכנית שירות זו, הוצא את הדיסקט והמשך לשלב קדם-ההתקנה הבא.

איסוף מידע

אסוף את המידע הבא להכנת ההתקנה של Windows 2000 :

- קרא את כל התיעוד המתייחס להתקנת Windows 2000 למידע עדכני על התקנה. עיין בקבצים txt. ו-doc. רלוונטיים הנמצאים בתקליטור ההתקנה Windows 2000 Server.
- ודא שברשותך כל הדיסקטים, הגדרות התצורה והתיעוד של מנהלי ההתקנים עבור חומרת צד-שלישי.
- ודא זמינות תקליטור ההתקנה של Windows 2000 Server, או זמינות שיתוף קבצי ההתקנה ברשת.
- (אופציונלי) פרמט ארבעה דיסקטים "3.5 בעלי קיבולת 1.44MB (אם אתה יוצר דיסקטים Setup Startup אופציונליים).

חשוב הדיסקטים של תוכנית ההתקנה של Windows NT 4.0 **אינם תואמים** Windows 2000.

דרישות סף לחומרה

עליך להיות מצוי בדרישות הסף לחומרה עבור התקנת Windows 2000 Server כך שתוכל לקבוע אם המערכת שברשותך מתאימה לדרישות אלה. דרישות הסף להתקנת Windows 2000 מפורטות בטבלה להלן.

רכיב	דרישת סף
מעבד	32-bit Pentium 133MHz
שטח דיסק פנוי	דיסק קשיח אחד או יותר בו %systemroot% (מיקום ברירת מחדל C:\WINNT) נמצא במחיצה בגודל מינימלי של 2GB, בה לפחות 671MB שטח דיסק פנוי.
זיכרון	128MB
תצוגה	צג VGA ברזולוציה של 480 × 640 (מומלץ 768 × 1024).
כונן תקליטורים	12×, אך מומלץ מהיר יותר; לא נדרש עבור התקנה דרך הרשת.
כוננים נוספים	כונן "3.5 בנפח 1.44MB לפחות, אלא אם חומרת המחשב מאפשרת אתחול והפעלת תוכנית ההתקנה מכונן התקליטורים (אפשרות הקיימת ברוב המחשבים).
רכיבים אופציונליים	עכבר או התקן הצבעה אחר. עבור התקנה מהרשת: מתאם רשת ומערכת הפעלה לרשתות מבוססת MS-DOS, המאפשרת התחברות לשרת המכיל את קבצי ההתקנה של Windows 2000.

תאימות חומרה

תוכנית ההתקנה של Windows 2000 בודקת את החומרה והתוכנה באופן אוטומטי ומדווחת על התנגשויות אפשריות. אולם, להבטחת התקנה מוצלחת עליך לוודא שחומרת המחשב שלך תואמת את Windows 2000 Server לפני התחלת הליך ההתקנה. כדי לבדוק זאת, ודא שהחומרה שלך מופיעה ברשימה HCL (**H**ardware **C**ompatibility **L**ist, רשימת תאימות חומרה). רשימת HCL נמצאת בתקליטור ההתקנה של Windows 2000, בתיקיה SUPPORT (שם הקובץ HCL.DOC). HCL היא רשימת כל החומרות שעברו בחינות תאימות חומרה (**H**ardware **C**ompatibility **T**ests - HCT). הרשימה גם מציינת איזה התקני חומרה נתמכים על ידי Windows 2000 Server. הבדיקות מתבצעות ב- WHQL (**W**indows **H**ardware **Q**uality **L**abs) וגם על ידי מספר ספקי חומרה. התקנת Windows 2000 Server במחשב בו חומרה שאינה מופיעה ברשימת HCL, עלולה להיכשל.

הערה Microsoft מעדכנת את רשימת HCL באופן קבוע. ניתן לעיין ברשימה העדכנית ביותר של חומרה נתמכת, באתר **Microsoft** בכתובת: **http://www.microsoft.com/hcl**.
אם כתובת זו אינה זמינה, נסה את הכתובת:
http://www.microsoft.com/isapi/redir.dll?prd=Win2000HCL&pver=1. כתובת זו אמורה לכוון לאתר WHQL. אם אתר WHQL אינו מופיע, חפש בכתובת:
http://www.microsoft.com באמצעות מילת המפתח **HCL**.

חומרה נחשבת "נתמכת" אם היא מופיעה ברשימת HCL והנך משתמש במנהל התקנים המסופק על ידי Microsoft לשליטה על החומרה. המונח "לא נתמך" אינו מעיד על האיכות היחסית של החומרה או מנהל ההתקנים שסופק על ידי צד-שלישי. מחשבים ומנהלי התקנים לא-נתמכים רבים עובדים כנדרש עם Windows 2000. אולם, צוות התמיכה של Windows 2000 ב- Microsoft אינו מציע שירותי תמיכה מלאים לבעיות ייחודיות לחומרה או מנהלי התקנים שאינם נתמכים.

Microsoft תומכת רק בהתקנים המופיעים ברשימת HCL. אם אחד מרכיבי המחשב אינו מופיע ברשימת HCL, התקשר ליצרן ההתקן ובקש מנהל התקנים עבור Windows 2000, אם קיים.

מחיצות דיסק

תוכנית ההתקנה של Windows 2000 מאפשרת התקנת Windows 2000 Server במחיצה (Partition) קיימת, או יצירת מחיצה חדשה והתקנת Windows 2000 במחיצה החדשה. בעת ההתקנה, תוכנית ההתקנה בודקת את הדיסק הקשיח. בהתאם למצב הדיסק, יוצעו חלק מאפשרויות החלוקה הבאות בעת ההתקנה:

- ❖ אם אין מחיצות כלל בדיסק, עליך ליצור ולהגדיר את מימדי מחיצת ההתקנה.
- ❖ אם יש כבר מחיצות בדיסק, ויש מספיק שטח דיסק פנוי (unallocated) ללא מחיצות, תוכל ליצור ולהגדיר את מימדי המחיצה, תוך שימוש בחלק זה של הדיסק שאינו מחולק.
- ❖ אם קיימת מחיצה גדולה דיה, תוכל להתקין את Windows 2000 Server במחיצה זו.
- ❖ אם קיימת מחיצה בדיסק, תוכל למחוק אותה, כדי ליצור שטח דיסק בלתי מחולק נוסף, ולהשתמש בו ליצירת מחיצת ההתקנה עבור Windows 2000.
- ❖ אם תעשה פעולה שתגרום למחיקת נתונים כלשהם, תתבקש לאשר את בחירתך. אם תמחק מחיצה קיימת, תגרום לכך שכל הנתונים במחיצה זו יימחקו אף הם. התקנת Windows 2000 במחיצה בה קיימת מערכת הפעלה NT אחרת, בתיקיה בשם Winnt, תגרום לשכתוב מערכת ההפעלה האחרת. אלא אם כן תגדיר שם שונה לתיקיית המערכת בזמן ההתקנה.

אף שתוכל להשתמש בתוכנית ההתקנה של Windows 2000 ליצירת מחיצות אחרות, עליך ליצור ולהגדיר את מימדי מחיצת ההתקנה בלבד. לאחר התקנת Windows 2000, השתמש בכלי Disk Management לחלק את יתרת שטח הדיסק שטרם נחלק למחיצות.

קביעת מימדי מחיצת ההתקנה

תוכנית ההתקנה של Windows 2000 Server דורשת מחיצת אתחול (Boot Partition) בגודל 2GB עם 671MB פנויים לפחות להתקנת קבצי מערכת ההפעלה של Windows 2000. אולם, מומלץ לפנות שטח דיסק גדול יותר במחיצת האתחול, כדי לאפשר התקנה עתידית של קבצים ותוכנות, כגון קובץ ההחלפה (Page File), כלי מערכת ההפעלה ועדכונים עבורה. מחיצת האתחול מכילה את קבצי הליבה של מערכת ההפעלה.

מחיצת המערכת (System Partition) מכילה את הקבצים הנדרשים לאתחול (Boot) הטעינה הראשונית של Windows 2000. במחשבים המבוססים על מעבדי x86, מערכת ההפעלה מאתחלת ממחיצת המערכת. המשמעות היא שמערכת Windows 2000 מחפשת קבצים מסוימים, כגון Ntldr, Ntdetect.com ו-Boot.ini בספריית השורש, בדרך כלל כונן :C (דיסק 0) בעת הפעלת המחשב. מערכת ההפעלה לא יכולה להתחיל אלא אם מחיצת המערכת מוגדרת כפעילה (Active).

שים לב המושגים Boot Partition (מחיצת אתחול) ו- System Partition (מחיצת המערכת) אינם זהים. החלק המבלבל הוא שה- System Partition היא המחיצה ממנה מתבצע תהליך האתחול (Boot) של המערכת. זה מבלבל ואתה עשוי להישאל על כך בבחינה.

מחיצת האתחול (Boot Partition) היא מקום ההתקנה של Windows 2000 Server. היא מכילה את ספריית האב של מערכת ההפעלה (ברירת מחדל Winnt), את תת התיקיה \System32, ליבת Windows 2000, וכל שאר הקבצים הנדרשים להפעלת מערכת ההפעלה. אם מערכת Windows 2000 Server מותקנת במחיצה פעילה (Active Partition), היא מהווה את מחיצת האתחול ומחיצת המערכת גם יחד.

מחיצת הדיסק בה תאחסן את קבצי Windows 2000 חייבת להיות מחיצה קבועה על הדיסק הקשיח, ועליה להיות בעלת שטח דיסק פנוי מספיק לאחסון כל הקבצים. יש לפרמט מחיצה זו באמצעות NTFS או באמצעות מערכות קבצים FAT16 או FAT32. אולם, לא ניתן להתקין Windows 2000 למחיצת FAT16 או FAT32 הדחוסים באמצעות תוכנות כמו Microsoft DriveSpace.

הערה ב-Windows 2000, אם תבחר לפרמט NTFS בעת ההתקנה, המחיצה תפורמט ישירות ל-NTFS. בגרסאות קודמות, פורמטה המחיצה למערכת הקבצים FAT ואז הוסבה ל-NTFS. הליך חדש זה מאפשר יצירת מחיצות גדולות מ- 4GB.

קבצי הפעלת ההתקנה, Winnt.exe ו-Winnt32.exe, מדווחים על שגיאה אם שטח הדיסק הפנוי קטן מדי (קטן מ- 671MB), או אם השטח הפנוי של הדיסק המוגדר עם Switch (מתג) /t: או /tempdrive: קטן מדי. אם אירעה שגיאה כזו, עליך לפנות שטח דיסק כנדרש ולהפעיל את Winnt או Winnt32 שנית.

Windows 2000 מחפשת קבצים מסוימים בספריית השורש של המחיצה הפעילה בעת הפעלת המחשב; אולם, ניתן להתקין את מערכת ההפעלה Windows 2000 על כונן אחר, כגון כונן D, כל עוד לכונן תצורה בעלת מערכת קבצים נתמכת. אם אתה רוצה

שלמחשב שלך תהיה יכולת אתחול כפול (Dual Boot) למערכות הפעלה שאינן תומכות ב-NTFS, כגון Windows 98, כונן C חייב להיות FAT16 או FAT32.

אם הדיסק הקשיח של מערכת ההפעלה כולל מחיצות שנשלטות על ידי BIOS, קבצי רשת אחרים כמו **N**etwork **S**ystem **F**iles (NFS), Stripe Sets, Volume Sets או שיקופים (Mirror), הם יופיעו על מסך ההתקנה כמחיצות מסוג בלתי מוכר. כדי למנוע מחיקה בשוגג של מרכיבים אלה, אין להשתמש בתוכנית ההתקנה למחיקת מחיצות המוצגות כבלתי מוכרות.

אם אתה מתקין עותק חדש של Windows 2000 במחיצה המשוקפת (Mirrored) בתוכנה, עליך לבטל את השיקוף לפני הפעלת תוכנית ההתקנה ולחזור ולהפעיל אותו לאחר השלמת ההתקנה. אולם, אם אתה משדרג Windows NT Server מגרסאות 3.51 או 4.0 או Windows 2000 Server, תוכל להשאיר את שיקוף הדיסקים פעיל, גם בעת ההתקנה.

אין להתקין Windows 2000 או לשדרג ל-Windows 2000 בכונן דחוס, אלא אם הדחיסה בוצעה על ידי תוכנית שירות דחיסת כוננים של NTFS. בטל דחיסת volume במערכת Windows 9x שנדחס באמצעות DriveSpace או DoubleSpace לפני הפעלת תוכנית ההתקנה של Windows 2000 על הכונן.

אם אתה מגדיר תצורת אתחול כפול של Windows 2000 יחד עם מערכת הפעלה אחרת, כגון MS-DOS, Windows 3.0, Windows 95, Windows 98, או Windows NT, התקן את Windows 2000 במחיצה נפרדת משלה. אף כי ניתן להתקין Windows 2000 במחיצה בה כבר מותקנת מערכת הפעלה אחרת, מומלץ ביותר להתקין את Windows 2000 במחיצה נפרדת, כיון שתוכנית ההתקנה של Windows 2000 עלולה להחליף בתיקיה Program Files קבצים שהותקנו על ידי מערכות הפעלה אחרות.

מערכות קבצים

בעת הפעלת תוכנית ההתקנה של Windows 2000 בשטח דיסק שאינו מחולק למחיצות, אתה מתבקש לבחור את מערכת הקבצים שתשמש לפרמוט המחיצה. עליך לבחור באיזו מערכת קבצים להשתמש לפני התקנת Windows 2000 Server. Windows 2000 תומכת ב-NTFS ומערכת קבצים FAT. ישנן שתי מערכות קבצי FAT : FAT16 ו-FAT32.

NTFS - NT File System

Windows 2000 תומכת במערכת NTFS. זוהי מערכת קבצים עם כל היכולות הבסיסיות של FAT, ובנוסף תכונות אחסון מתקדמות כגון אבטחה, דחיסה ושדרוג קל יותר לנפחים גדולים. מערכות הפעלה Windows 2000 ו-Windows NT הן מערכות ההפעלה היחידות שתוכננו לגשת לנתונים הנמצאים על דיסק מקומי שפורמט עם NTFS.

הערה ישנן תוכניות שירות צד-שלישי שתוכננו לתת גישה למחיצות NTFS מ-MS-DOS ומערכות הפעלה אחרות; אולם, תוכניות שירות אלו אינן נתמכות על ידי Microsoft.

Windows 2000 מכילה גירסה חדשה של NTFS: NTFS 5.0. NTFS גירסה 5.0 מציעה שיפורי ביצועים רבים ותכונות חדשות, כולל מכסות דיסק לפי-משתמש, הצפנת קבצים, Reparse points (נקודות חלוקה). נקודות חלוקה משמשות להרחבת תכונות מערכת הקבצים. יישומים יכולים ללכוד פעולות פתוחות מול אובייקטים של מערכת קבצים ולבצע את הקוד שלהם לפני החזרת מענה של נתוני הקובץ (Reparse Points נידונות ביתר פירוט בפרק 4). תוכל גם להוסיף שטח דיסק NTFS version 5.0 volumes ללא אתחול מחדש.

NTFS דורשת Windows 2000 או Windows NT. אם המחשב איתחל תחת מערכת הפעלה אחרת, מערכת הפעלה זו לא תוכל לגשת למחיצות NTFS (מטעמי אבטחה).

עליך להשתמש ב-NTFS כאשר מחיצת Windows 2000 דורשת אחת מהתכונות הבאות:

- **אבטחה מקומית ברמת הקובץ וברמת התיקיה** – NTFS מאפשרת בקרת גישה לקבצים ותיקיות בין אם הגישה היא מקומית או מהרשת (ב-Windows 9x האבטחה היא ברמת הרשת בלבד).
- **דחיסת דיסקים** – NTFS דוחסת דיסקים לאחסון יותר נתונים במחיצה.
- **מכסות דיסק** – NTFS מאפשרת בקרת שימוש בדיסק על בסיס מכסה (Quota) למשתמש.
- **הצפנה** – NTFS מאפשרת הצפנת נתוני קובץ על הדיסק הפיסי עצמו.

ככלל, NTFS היא מערכת הקבצים המומלצת. היא היחידה התומכת במכלול Active Directory Services, הכולל תכונות חשובות רבות כגון Domains, ואבטחה מבוססת-Domains. אולם, ייתכן שיהיה צורך להשתמש במחיצות FAT16 ו-FAT32 במצבים מסוימים של אתחול כפול. אם בכוונתך לקדם שרת להיות Domain Controller, אתה נדרש לפרמט את מחיצת ההתקנה עם NTFS.

FAT16 ו-FAT32

מערכות קבצים FAT16 ו-FAT32 מאפשרות גישה על ידי, ותאימות עם, יותר ממערכת הפעלה אחת. כדי לאתחל את המחשב עם Windows 2000 ועם מערכת הפעלה אחרת, מחיצת המערכת של Windows 2000 חייבת להיות מפורמטת עם מערכת קבצים FAT16 או FAT32. אם בחרת FAT והמחיצה קטנה מ- 2048MB, תוכנית ההתקנה תפרמט את המחיצה כ-FAT16. במחיצות הגדולות מ- 2GB, תוכנית ההתקנה תפרמט אוטומטית את הדיסק הקשיח ל-FAT32.

הערה Windows 2000 **תומכת ב**-volumes **של** FAT32 **בגודל כלשהו שנוצרו על ידי** Windows 95 OSR2 **או** Windows 98. **אולם,** Windows 2000 **תפרמט** FAT32 volumes **רק עד גודל של** 32GB. **מגבלה זו נובעת ממגבלות זיכרון תוכניות שירות להתאוששות, כגון** Autochk.

FAT16 ו-FAT32 אינן מציעות רבות מן התכונות הנתמכות על ידי NTFS, כגון אבטחה ברמת הקובץ. אי לכך, ברוב המצבים יש לפרמט את הדיסק הקשיח עם NTFS. הסיבה היחידה להשתמש ב-FAT16 או FAT32 היא אתחול כפול. אם אתה מכין מחשב לאתחול כפול, עליך לפרמט רק את מחיצת המערכת כ-FAT16 או FAT32. לדוגמה, אם כונן C הוא מחיצת המערכת, תוכל לפרמט את כונן C כ-FAT16 או FAT32 ולפרמט את כונן D כ-NTFS. אולם, Microsoft אינה ממליצה על אתחול כפול בשרת.

שיקולי מערכת קבצים

אם מחיצת המערכת (System Partition) ומחיצת האתחול (Boot Partition) הן שתי מחיצות שונות, תוכנית ההתקנה של Windows 2000 תפרמט רק את מחיצת האתחול (Boot Patrition) כברירת מחדל. עליך לבצע פעולות נוספות בעת ההתקנה כדי לפרמט גם את מחיצת המערכת (System Partition). הטבלה וההנחיות להלן יסייעו בהחלטה איזו מערכת קבצים מתאימה למחיצת האתחול שלך.

- ניתן להשתמש במחיצה קיימת שכבר פורמטה. כברירת המחדל נשמרת מערכת הקבצים הקיימת, תוך שהיא שומרת את כל הקבצים במחיצה זו.
- ניתן להסב מחיצת FAT קיימת ל-NTFS כדי לנצל את תכונות האבטחה ותכונות משופרות נוספות של מערכת הקבצים Windows 2000. אפשרות זו שומרת על קבצים קיימים, אך רק ל-Windows 2000 תהיה גישה למחיצה זו.
- ניתן לפרמט מחיצה קיימת ל-NTFS או למערכת קבצים FAT. פעולת הפורמט מוחקת את כל הקבצים הקיימים במחיצה זו. זכור שרק ל-Windows 2000 ו-Windows NT תהיה גישה למחיצה המפורמטת כ-NTFS.
- עליך לבחור אפשרות FAT אם מחיצת האתחול שלך קטנה מ- 2GB ואתה רוצה לאפשר גישה למחיצה זו בעת הפעלת MS-DOS, Windows 3x, Windows 95, Windows 98, או 0S/2 במחשב זה. תוכנית ההתקנה תפרמט את הדיסק עם FAT.
- עליך לבחור באפשרות FAT אם אתה מבצע אתחול כפול עם גרסת OSR2 של Windows 95 או Windows 98, או Windows NT ויש לך מחיצת אתחול גדולה מ- 2GB. תוכנית ההתקנה תפרמט את הדיסק עם FAT32.
- עליך לבחור את אפשרות NTFS אם המערכת פועלת תחת Windows 2000 וברצונך לנצל את היתרונות של NTFS (עיין בטבלה להלן). תוכנית ההתקנה תפרמט את מחיצת האתחול עם גירסה 5.0 של NTFS.

הערה **לא ניתן להסב** FAT16 volumes **למחיצות** FAT32 **ב-**Windows 2000.

הטבלה להלן משווה בין התכונות השונות של שלוש מערכות הקבצים הנתמכות על ידי Windows 2000.

מערכת הפעלה	FAT16	FAT32	NTFS
תאימות כוללת	מוכר על ידי MS-DOS, Windows 95, Windows 98, Windows NT, Windows 2000, ו-OS/2.	מוכר רק על ידי Windows 95 גירסה OSR2, Windows 98, ו-Windows 2000.	מוכר על ידי Windows NT ו- Windows 2000. כאשר המחשב פועל תחת מערכת הפעלה אחרת (כמו MS-DOS, Windows 95, Windows 98, או OS/2), למערכת הפעלה זו לא תהיה גישה לקבצים ב- NTFS Volumes באותו מחשב.
נתמך על ידי MS-DOS ו-Windows 3x	כן	לא	לא
נתמך על ידי גרסאות Windows 95 הקודמות לגרסת OSR2	כן	לא	לא
נתמך על ידי Windows 95 גרסת OSR2 ו- Windows 98	כן	כן	לא
נתמך על ידי Windows NT 3.51	כן	לא	כן, אבל Windows NT 3.51 אינו תומכת בגירסה 5.0 של NTFS.
נתמך על ידי Windows NT 4.0	כן	לא	כן. Windows NT 4.0 תומכת בגירסה 5.0 של NTFS אם מותקן Service Pack 4 או יותר.
נתמך על ידי Windows 2000	כן	כן	כן

הערה ככל הידוע, Windows 95 בגרסת OSR2 לא הופצה מעולם מחוץ לארה"ב. ההתייחסות לגירסה זו בספר נובעת רק מכיון שאתה עשוי (עלול) להשאל על כך בבחינה.

רשיונות

Windows 2000 Server תומכת בשני סוגים של רשיונות: לפי-שרת (Per Server) ולפי-מושב (Per seat) - לפי משתמש/תחנת עבודה. במצב לפי-שרת, מוקצים לשרת רשיונות גישה ללקוח (**C**lient **A**ccess **L**icenses - CAL). במצב לפי-מושב, כל מחשב שניגש למחשב Windows 2000 Server חייב CAL נפרד.

Per Server License

בהקצאת רשיונות לפי שרת (Per Server License), CAL (רשיונות גישה ללקוח) מוקצים לשרת מסוים. כל CAL מאפשר חיבור בודד לשרת עבור כל מחשב לקוח, לקבלת פעולות רשת בסיסיות. נדרש שכמות ה-CAL הייעודי לשרת יהיה לפחות כמספר המירבי של מחשבי הלקוח העשויים להתחבר בו-זמנית לאותו שרת.

דוגמה במידה וקנית רשיון לפי שרת של 300 מחשבים, תוכל לחבר עד 300 מחשבים בו-זמנית לאותו שרת דרך הרשת. המחשב ה-301 שינסה להתחבר - בקשתו תידחה. שים לב שרשיון לפי שרת קובע את מספר החיבורים הנערכים בו-זמנית, כך שאתה יכול, תיאורתית, לקנות רשיון של 300 לפי שרת גם אם בחברה שלך יש 500 מחשבים, אך דע לך שרק 300 מהם יצליחו להתחבר בו-זמנית דרך הרשת.

שיטת רשיונות לפי שרת מועדפת על ידי חברות קטנות להן רק מחשב אחד המפעיל Windows 2000 Server. היא גם יעילה לשרתי אינטרנט או שרתי גישה-מרחוק כאשר ייתכן שלמחשבי לקוחות אין רשיון רשת לקוח Windows 2000. במצב זה, רשיון לפי שרת מאפשר להגדיר מספר חיבורי שרת בו-זמניים ולדחות כל ניסיון התחברות נוסף.

הערה אם אינך בטוח באיזה סוג רשיון לבחור, בחר ברשיון לפי שרת. זאת, מכיון שניתן לשנות, פעם אחת בלבד, מרשיון לפי שרת לרשיון לפי מושב ללא תוספת תשלום (על ידי לחיצה כפולה על הסמל Licencing בלוח הבקרה). אין צורך להודיע ל- Microsoft על ביצוע שינוי זה. זה הוא שינו חד-כיווני; לא ניתן לשנות מרשיון לפי מושב לרשיון לפי שרת.

Per-Seat License

מצב רשיון לפי מושב (Per-Seat License) דורש CAL (רשיונות גישה ללקוח) עבור כל מחשב לקוח המשמש לגישה ליישומי רשת בסיסיים של Windows 2000 Server. לאחר שלמחשב לקוח יש CAL, ניתן להשתמש בו לגשת לכל מחשב המפעיל Windows 2000 Server ברשת. לעיתים קרובות רשיון לפי מושב הוא כלכלי יותר לרשתות גדולות, בהם מחשבי לקוחות ישמשו להתחברות ליותר משרת אחד.

בשירותי Terminal (מסופים), הרשיון הוא בדרך כלל לפי מושב, פרט לרשיון Terminal Services Internet Connector (חיבור אינטרנט דרך שירות מסופים) שבו

תמיד ישמש מצב רשיון לפי שרת. אם בכוונתך להשתמש בשירותי Terminal (מסופים), עליך להתקין שני רכיבים: Terminal Services (שירותי מסופים) ו- Terminal Services Licensing (רשיון לשירותי מסופים).

הערה ברשיון **לפי מושב** (Per-Seat License), הרשיון **שייך** לתחנת העבודה **ובעזרתו** היא יכולה להתחבר לכל שרת ברשת **ואפילו** למספר שרתים בו-זמנית. אפשר לדמות את Per-Seat License כמו תגית איתה ניתן להיכנס למספר מקומות.

(**Cl**ient **A**ccess **L**icense) CAL

CAL (**C**lient **A**ccess **L**icense) נותן למחשבי לקוח את הזכות להתחבר למחשבים המפעילים Windows 2000 Server, כך שמחשבי לקוח יכלו להתחבר לשירותי רשת, תיקיות משותפות, ומשאבי הדפסה. בעת התקנת Windows 2000 Server עליך לבחור CAL מתאים: Per Server License או Per Seat License. השירותים הבאים **אינם** דורשים CAL:

- ❖ גישה אנונימית או מאומתת ל-Windows 2000 Server באמצעות שירות IIS - Microsoft **I**nternet **I**nformation **S**ervices גירסה 4.0, או יישום Web-Server (שרת-אינטרנט) המספק שיתוף בקבצי HTML (**H**yper**t**ext **M**arkup **L**anguage) באמצעות פרוטוקול HTTP (**H**yper**t**ext **T**ransfer **P**rotocol).
- ❖ חיבורי Telnet ו- FTP (**F**ile **T**ransfer **P**rotocol).

הערה אם הארגון שלך משתמש במוצרי Microsoft BackOffice, **חובה** שיהיו לך רשיונות גם **למוצרי** BackOffice. רשיון Windows 2000 **אינו** מכסה את **מוצרי** BackOffice.

Workgroups and Domains

בעת ההתקנה, עליך לבחור את סוג הרשת אליה יתחבר המחשב שלך. מחשב הפועל תחת Windows 2000 יכול להצטרף לאחד משני סוגים של רשתות: Workgroups (קבוצות עבודה) או Domains (תחומים).

הצטרפות ל- Workgroup

בעת הצטרפות לקבוצת עבודה, הקצה שם קבוצת עבודה למחשב. שם קבוצת העבודה יכול להיות שמה של קבוצת עבודה קיימת או שם של קבוצת עבודה שנוצרה בעת ההתקנה. בין אם הקצת שם קבוצת עבודה חדש או השתמשת בשם קיים, המחשב יופיע כחבר בקבוצה זו כאשר משתמשים במחשבים אחרים ידפדפו ברשת לאיתור משאבי רשת. Domain ו-Workgroup יכולים להיות בעלי שם זהה, אך קח בחשבון את השיקולים הבאים:

- ❖ מחשבי קבוצת העבודה אינם חברים ב-Domain ואינם כלולים במערך ניהול ה-Domain.
- ❖ ב-Windows 2000 Explorer (סייר), מחשבי קבוצת העבודה מופיעים יחד עם מחשבי ה-Domain.

הצטרפות ל- Domain

בעת ההתקנה, אשף ההתקנה של Windows 2000, מספק גישה להתחברות ל-Domain (תחום) קיים. האשף משתמש לקבלת שם DNS של ה-Domain. לפני שמחשב הפועל תחת מערכות הפעלה Windows NT או Windows 2000 יוכל להצטרף ל-Domain (תחום), יש ליצור או להוסיף חשבון מחשב למסד הנתונים של ה-Domain. רק משתמשים בעלי הרשאת Join A Computer To The Domain יכולים ליצור חשבון למחשב. לחברים בקבוצות Administrators, Domain Administrators או Account Operators, יש הרשאה כזו כברירת מחדל. אפשרויות פתיחת חשבון מחשב ב-Domain :

- לפני ההתקנה ליצור חשבון מחשב ב- Domain Controller. או,
- בזמן ההתקנה ליצור חשבון מחשב על ידי הקלדת שם וסיסמה של משתמש בעל הרשאה מתאימה (בדרך כלל Administrator).

בעת התחברות ל-Domain, צור חשבון מחשב למחשב זה מראש, או צור אותו בהליך ההתקנה על ידי סימון תיבת הסימון Create A Computer Account In The Domain. עתה, ספק חשבון משתמש וסיסמה של משתמש שבסמכותו להוסיף חשבונות מחשב ל-Domain. כברירת מחדל, חשבון זה חייב להיות חשבון מנהל (Administrator).

הערה בעת התחברות ל-Domain, אף אם חשבון המחשב נוצר קודם, יש לספק אישורי Domain.

לפחות DC (בקר תחום) אחד ושרת DNS אחד חייבים להיות מקוונים (Online) בעת התקנת מחשב ב-domain. אם התקנת את Windows 2000 Server כשרת עצמאי בלי חיבור ל-Domain, תוכל להצטרף ל-Domain מאוחר יותר על ידי שימוש בכרטיסיה Network Identification בתיבת הדו-שיח System Properties, כמתואר בתרשים 2.1.



תרשים 2.1 הכרטיסיה Network Identification בתיבת הדו-שיח System Properties.

שדרוג או התקנה חדשה

לפני הפעלת תוכנית ההתקנה של Windows 2000 Server, עליך להחליט אם ברצונך לשדרג את ההתקנה הקיימת של Windows NT או לבצע התקנה חדשה.

Upgrading (שדרוג) הוא הליך של התקנת Windows 2000 Server בתיקיה המכילה גירסה כלשהי של Windows NT. שדרוג מתקין את Windows 2000 Server באותה תיקיה בה מותקנת מערכת ההפעלה הנוכחית. גרסאות Windows NT מהן ניתן לשדרג הן:

- ❖ Windows NT Server 3.51.
- ❖ Windows NT Server 4.0 Server או Windows NT 4.0 Terminal Server.

אם ברשותך Windows NT 4.0 Server Enterprise Edition, תוכל לשדרג למערכת Windows 2000 Advanced Server, אך לא למערכת Windows 2000 Server. אם ברשותך גרסת Windows NT Server מוקדמת מגירסה 3.51, לא תוכל לשדרג ישירות ל-Windows 2000 Server; עליך קודם לשדרג ל- Windows NT Server 3.51/4.0. את Windows NT Workstations (תחנות עבודה Windows NT) ו-Windows 2000 Professional לא ניתן לשדרג ל- Windows 2000 Server.

Installing (התקנה), בניגוד לשדרוג, הוא הליך של הכנסת מערכת ההפעלה לתיקיה חדשה, מחיקת מערכת ההפעלה הקודמת בעת ההתקנה, או התקנת Windows 2000 Server על דיסק או מחיצת דיסק שאין בה מערכת הפעלה קודמת. אם ברצונך לבצע התקנה חדשה במחיצת דיסק שבה יישומים שברצונך לשמור, יש לגבות אותם ולחזור להתקינם מחדש לאחר התקנת Windows 2000 Server.

אם ברצונך לבצע התקנה חדשה של Windows 2000 Server במחיצה שהכילה בעבר Windows 2000 Server, ויש לך מסמכים בתיקיה My Documents שברצונך לשמור, גבה את המסמכים בתיקיה Documents and Settings והעתק את המסמכים חזרה לתיקיה לאחר השלמת ההתקנה. התיקיה My Documents מצביעה לעבר תת-תיקיות שמתחת לתיקיה Documents and Settings.

שיטות התקנה

קיימות שלוש שיטות להתקנת Windows 2000 Server על פלטפורמת Intel:

- ❖ באמצעות דיסקטים.
- ❖ תקליטור.
- ❖ דרך הרשת.

התקנה מדיסקטים

Windows 2000 Server נמכרת על גבי תקליטור וכוללת גם ארבעה דיסקטים להתקנה. דיסקטים אלה נדרשים אם הנך מתקין את Windows 2000 Server על מחשב מבוסס מעבד x86, שאינו מפעיל מערכת הפעלה MS-DOS או Windows ואשר החומרה שלו אינה מאפשרת אתחול מכונן התקליטורים. דיסקטים אלה גם מאפשרים הפעלת Windows 2000 מאוחר יותר, כאשר ייתכן שהיא לא תוכל לפעול מעצמה עקב שגיאת מחשב, וליזום תיקון חירום.

תוכל ליצור דיסקטים להתקנה על ידי הפעלת קובץ Makeboot.exe או Makebt32.exe מהתיקיה Bootdisk\ שבתקליטור ההתקנה של Windows 2000 Server. Makeboot.exe הוא יישום DOS בן 16 סיביות הפועל על מערכות הפעלה MS-DOS, מערכות הפעלה 16 סיביות כגון Windows 3.11, ועל Windows 9x. Makebt32.exe הוא יישום 32 סיביות הפועל על Windows NT ו-Windows 2000.

לאחר הטעינה הראשונית בעת ההתקנה, Windows 2000 תתחיל לפעול ושאר ההתקנה תפעל תחת Windows 2000, דבר המסייע באיתור תקלות. לדוגמה, הליך ההתקנה יציג קוד בדיקת שגיאה Windows 2000 סטנדרטי אם ארעה שגיאה בעת ההתקנה.

להתחלת ההתקנה של Windows 2000 Server באמצעות הדיסקטים, כבה תחילה את המחשב, הכנס את הדיסקט עם התווית Windows 2000 Setup Boot Disk לכונן A, והפעל את המחשב שנית. תוכנית ההתקנה תתחיל באופן אוטומטי.

הערה אם ההתקנה היא על מחשב Windows 2000 Server **בו אין** מערכת הפעלה קודמת, **ואם** הנך משתמש בדיסקט אתחול MS-DOS (**ומבצע** התקנה דרך הרשת), עליך לפרמט את **הכונן** תחילה. אולם, אם הנך משתמש בדיסקטים של Windows 2000 להתחלת **תוכנית** ההתקנה, **תוכל** לפרמט את **הכונן תוך** כדי התקנה.

בעת הטעינה מהדיסקטים של אתחול ההתקנה, הסרגל בתחתית המסך מציג את רכיבי Windows 2000 הנטענים. רכיבים אלה מתוארים בסעיפים הבאים.

Setup Disk 1

הקובץ Setupldr.bin מתחיל את ההתקנה. המחשב נבדק ונאספים נתונים מזהים אודותיו. אם לא נמצא מנהל התקנים עבור הדיסק הקשיח המכיל את מחיצת האתחול, ייתכן שתיאלץ לטעון מנהל התקנים של צד-שלישי. עקוב אחר הוראות ההתקנה בתוכנית וטען מנהל התקן עבור בקר SCSI או RAID. בשלב זה נטען גם חלק הטקסט (Text Mode) של Windows 2000 Setup. קובץ Ntkrnlmp.exe טוען את Windows 2000 Executive.

Setup Disk 2

דיסקט זה טוען את HAL, כלי הגדרת תצורה, גופנים, נתונים ייחודיים-מיקום (Locale-Specific), מנהלי התקנים ובקרים. תוכנית ההתקנה של Windows 2000 ממשיכה לפעול במצב טקסט.

Setup Disk 3

דיסקט זה טוען את אשכול מנהלי אשכול כונני Compaq ומנהלי ההתקן של בקרי הדיסקים. במהלך פעולה זו, תוכנית ההתקנה מאתרת את מנהלי ההתקן המתאימים עבור המערכת וטוענת את Dynamic Volume Support - dmboot1. תוכנית ההתקנה של Windows 2000 תמשיך לפעול במצב טקסט.

Setup Disk 4

דיסקט זה טוען את מנהלי ההתקנים של הדיסקטים, של כונן תקליטורים SCSI, ודיסקים קשיחים, מנהלי התקנים של קבצי מערכת - File System Drivers (FAT, NTFS ו-CDFS). Windows 2000 נטענת ומשתלטת על הליך ההתקנה. מסך Welcome (ברוכים הבאים) מופיע, ותוכל לבחור אם להתקין את Windows 2000, לתקן גירסה קיימת של Windows 2000, או לצאת מתוכנית ההתקנה. בשלב זה התוכנית ניגשת לכונן התקליטורים. תוכנית ההתקנה מנסה לאתר גרסאות קודמות של Windows ומחיצות כלשהן. תוכל למחוק מחיצות קיימות וליצור חדשות. לאחר הגדרת המחיצות, עליך לבחור מערכת קבצים (NTFS או FAT). לאחר בחירה זו המערכת מפרמטת את המחיצה. עם סיום הפרמוט, מתחיל הליך העתקת הקבצים. לאחר השלמת ההעתקה, המערכת מאתחלת מחדש. הוצא את כל הדיסקטים מהכוננים לפני האתחול החדש.

אחרי Setup Disk 4

לאחר האתחול החוזר, תוכנית ההתקנה של Windows 2000 מתחילה במצב ממשק המשתמש הגרפי (GUI). קבצים מהתקליטור ממשיכים להיות מועתקים לדיסק הקשיח. תוכנית ההתקנה מאתרת ומתקינה התקנים ומבקשת נתונים מהמשתמש. עליך לבחור איזה רכיבים להתקין. עתה, בחר את אופן התקנת הרשת - Typical (רגילה) או Custom (מותאמת אישית) וסוג הרשת אליה תרצה להתחבר - Workgroup (קבוצת עבודה) או Domain (תחום). תוכנית ההתקנה בונה את רשימת הקבצים, מתקינה ומגדירה את הרכיבים.

הערה בדרך כלל לא נעשה שימוש בדיסקטים אלו מאחר וכמעט כל המחשבים המיועדים להיות שרת תומכים באתחול מכונן התקליטורים.

תקליטור אתחול

אם קבצי ההתקנה של Windows 2000 Server שלך הם על תקליטור, וה-BIOS שלך תומך באתחול מתקליטור - Bootable CD-ROM (ללא מצב הדמיה), הכנס את תקליטור Windows 2000 Server לכונן התקליטורים, וכבה את המחשב. כאשר תחזור ותפעיל את המחשב, תוכנית ההתקנה תתחיל אוטומטית.

כאשר תוכנית ההתקנה מבקשת הוצאת התקליטור מהכונן, עשה כן במערכות בעלות תקליטור לאתחול. אחרת, תוכנית ההתקנה תתחיל שוב מחדש באתחול הבא.

חשוב אף שהמערכת שלך עשויה לתמוך בתקליטור אתחול, ייתכן שתידרש לשנות את הגדרות BIOS המערכת כדי לאתחל מתקליטור.

אם המחשב שלך פועל תחת מערכות הפעלה Windows 95, Windows 98, או Windows NT, ואתה מכניס את תקליטור האתחול של Windows 2000 בעת שהמחשב פועל, תופיע תיבת הדו-שיח של אשף ההתקנות של Windows 2000 (בתנאי שלא ביטלת את האפשרות להפעלה אוטומטית, AutoPlay).

התקנה דרך הרשת (מבוססת שרת)

קבצי המערכת של Windows 2000 Server חייבים להיות זמינים דרך הרשת. העתק את תקליטור ההתקנה של Windows 2000, או לפחות את תיקיית המקור (\I386), לתיקיה על דיסק קשיח בשרת הרשת והגדר את התיקיה כשיתוף (Share). יצירה של תיקיית הפצה נידון ביתר פירוט בפרק 3.

שדרוג Windows 95, Windows 98, או Windows NT

אם מערכת ההפעלה הנוכחית המותקנת במחשב שלך היא Windows 95, Windows 98 או Windows NT, התחבר לקבצי המערכת דרך הרשת והפעל (לחץ לחיצה כפולה) את Winnt32.exe, הממוקם בתיקיה I386. ניתן לשדרג רק את Windows NT Server ל-Windows 2000 Server. לא ניתן לשדרג את מערכות ההפעלה האחרות ל-Windows 2000 Server. אם אתה מתקין Windows 2000 Server על מחשב Windows NT Server, המערכת תבקש ממך להתקין או לשדרג ל-Windows 2000 Server. בכל מקרה אחר אתה נדרש להתקין Windows 2000 Server.

שדרוג של Windows NT Server שומר על רוב הגדרות והעדפות המערכת, ורוב התקנות היישומים. אם תעדיף תצורת אתחול כפול, בחר באפשרות Install Windows 2000 Server. הקש Enter או על לחץ Next להמשך.

התקנה חדשה או שדרוג גירסה נוכחית

אם לא מותקנת Windows 95, Windows 98 או Windows NT במחשב שלך, עליך להפעיל MS-DOS ולקוח רשת MS-DOS, להקמת קשר עם תיקיית הרשת המשותפת המכילה את קבצי ההתקנה.

בעודך מפעיל MS-DOS network client (לקוח רשת של MS-DOS), התחבר לקבצי המערכת דרך הרשת והפעל קובץ Winnt.exe, הממוקם בשיתוף ברשת.

נדרשים 500KB פנויים של זיכרון קונבנציונלי להפעלה מוצלחת של שגרת ההתקנה. ודא שטעינת Emm386.exe ושטעינת את כל מנהלי ההתקנים בזיכרון העליון (High).

טיפ לפינוי עוד זיכרון, הפעל LoadHigh Winnt.exe לטעינת חלקים של Winnt.exe בזיכרון העליון.

מומלץ שקובץ Smartdrv.exe, יהיה פעיל, אחרת ההתקנה תהיה איטית ותארך בין ארבע ל- 12 שעות.

הערה לא מומלץ להתקין ברשת ממצב DOS. ההתקנה עשוייה להארך זמן רב יותר מאשר התקנה מתקליטור או דיסקטים.

בחירת רכיבים להתקנה

מערכת Windows 2000 Server כוללת מיגוון רחב של רכיבי ליבה, כולל מספר כלי ניהול המותקנים באופן אוטומטי על ידי תוכנית ההתקנה. בנוסף, תוכל לבחור בין מספר רכיבים המגדילים את התפקודיות של Windows 2000 Server. רכיבים אלה ניתן להתקין בזמן ההתקנה או להוסיפם מאוחר יותר (באמצעות האפשרות Add/Remove Windows Components שביישומון לוח הבקרה Add/Remove Programs).

בחירת יותר רכיבים, משמעה הענקת יכולות גבוהות יותר לשרת. אולם, בחר רק את הרכיבים הדרושים לך, כיון שכל רכיב צורך שטח דיסק נוסף. הטבלה הבאה תסייע לך בבחירת הרכיבים הדרושים להתקנה.

שימוש אפשרי של השרת	**רכיבים אופציונליים שיש לשקול התקנתם**
שרת DHCP, DNS, או WINS (ברשת TCP/IP)	**D**ynamic **H**ost **C**onfiguration **P**rotocol (DHCP), DNS, או **W**indows **I**nternet **N**ame **S**ervice (WINS) - כולם חלק משירותי הרשת.
ניהול רשתות מרכזי	כלי ניהול וניטור
אימות ותקשורת מאובטחת	• Internet Authentication Services (שירותי אימות באינטרנט) - חלק משירותי הרשת. • שירותי הרשאות (רשיונות)
גישה לקבצים	• Microsoft Index Service (שירות אינדקס של Microsoft) • אחסון מרוחק. • שירותי קבצים והדפסה רישתיים אחרים (תמיכה ב- NetWare, Macintosh, ו-Unix). מחשבי לקוח של NetWare נתמכים באמצעות שירותי **G**ateway **S**ervices for **N**et**w**are (GSNW). כלי Directory Service Migration Tool מתקין את GSNW אם שירותי **N**etWare **D**irectory **S**ervices (NDS) אינם מותקנים.
גישה להדפסות	שירותים אחרים של קבצי רשת ומדפסות (תמיכה ב-NetWare, Macintosh ו-Unix).
שירותי מסוף (Terminal Services)	• Terminal Services (שירותי מסוף) • Terminal Servicing Licensing (רישוי שירות מסוף)
תמיכה ביישומים	• Message Queuing Service (שירות תור הודעות) • **Q**uality **o**f **S**ervice (QoS) Admission Control Service (חלק משירותי הרשת)

שימוש אפשרי של השרת	רכיבים אופציונליים שיש לשקול התקנתם
תשתית אינטרנט (Web)	• **I**nternet **I**nformation **S**ervices - IIS • Site Server ו- Lightweight Access Protocol (חלק משירותי הרשת)
תמיכה בטלפון ופקס	Connection Manager Administration Kit ו- Connection Point Services (חלק מכלי הניהול והניטור)
תקשורת מולטימדיה	Windows Media Services
תמיכה במיגוון מערכות הפעלה של לקוחות	שירותי קבצים ומדפסות אחרים (תמיכה ב- NetWare, Macintosh ו-Unix).

הטבלה הבאה מתארת את הרכיבים האופציונליים ומיועדת לשימוש יחד עם הטבלה הקודמת לסייע בבחירת הרכיב המתאים להתקנה.

רכיב אופציונלי	תיאור
Certificate Services	מספק תמיכה בהרשאות, כולל דואר אלקטרוני מאובטח, אימות מבוסס-אינטרנט, ואימות באמצעות כרטיס חכם.
Internet **I**nformation **S**ervices	מספק תמיכה ליצירה, הגדרה וניהול אתרי אינטרנט, יחד עם **N**etwork **N**ews **T**ransfer **P**rotocol (NNTP, פרוטוקול העברת חדשות ברשת), FTP, ו- **S**imple **M**ail **T**ransfer **P**rotocol (SMTP, פרוטוקול העברת דואר רגיל)
כלי ניהול וניטור	• מספק כלים לניהול וניטור הרשת ובמיוחד כלי Network Monitor, מנתח Packets (מנות). כולל גם פרוטוקול **S**imple **N**etwork **M**anagement (SNMP). • כלי ניהול אחרים כולל תמיכה בחיוג לקוחות ועדכון ספרי טלפון של לקוחות, ותוכנת שירות להגירה מ-DNS ל-Windows Active Directory Services.
Microsoft Queuing Services	מספק שירותים שתומכים בהודעות הנדרשות על ידי יישומים מבוזרים, המאפשרות ליישומים אלה לתפקד באמינות ברשתות הטרוגניות או כאשר המחשב לא-מקוון זמנית.
Microsoft Indexing Services	מספק תפקידי אינדקס עבור מסמכים המאוחסנים על הדיסק, ובכך מאפשר למשתמשים לחפש טקסט או תכונות ייחודיים במסמכים.
Microsoft Script Debugger	מספק Script (תסריט) לתמיכה בפיתוח.

רכיב אופציונלי	תיאור
שירותי רשת	מספק תמיכה חשובה לרשת, כולל הפריטים שברשימה להלן: • COM Internet Services Proxy - תומך ביישומים מבוזרים המשתמשים ב- HTTP לתקשורת דרך IIS. • **D**omain **N**ame **S**ystem (**DNS**), מערכת שמות תחומים) מאחזר שמות עבור לקוחות הפועלים תחת Windows 2000. באמצעות אחזור שמות, משתמשים יכולים לגשת לשרתים לפי שם, במקום שיאלצו להשתמש בכתובות IP שקשה לזהות ולזכור. במילים אחרות הוא מקשר בין שם (אותו קל לזכור) לכתובת IP (אותה קשה לזכור). • **D**ynamic **H**ost **C**onfiguration **P**rotocol (**DHCP**, פרוטוקול הגדרה דינמית של מארח) - מספק לשרת יכולת דינמית להענקת כתובות IP למחשבים אחרים ברשת. כל מחשב ברשת זקוק לכתובת IP. כדי למנוע בעיות וטעיות הנובעות מהקצאה ידנית של כתובות IP לכל מחשב ברשת, וכדי לחסוך בעבודה מומלץ שהקצאת כתובות IP תעשה על ידי DHCP. עם DHCP אין צורך להגדיר ולתחזק כתובות IP על מחשבי אינטראנט כלשהם, פרט לאלה המספקים DHCP, DNS או WINS. • Internet Authentication Service (שירות אימות באינטרנט) - מספק אימות למשתמשים המתחברים באמצעות חיוג. • QoS Admission Control Service (בקרת כניסה ורוחב פס) - מאפשר בקרה על הקצאת רוחב פס ליישומים. יישומים חשובים מקבלים רוחב פס גדול יותר מיישומים חשובים פחות. • Simple TCP/IP Services - תומכים בשירותי Character Generator, Discard Daytime, Echo, ו- Quote of the Day. • Site Server ILS Service - תמיכה בישומיים טלפוניים המאפשרים גישה לתכונות כמו זיהוי מתקשר, שיחות ועידה, שיחות וידאו, ופקסים. תמיכה זו תלויה ב- IIS. • Windows Internet Naming Service מספק מערכת תמיכת שמות NetBIOS over TCP/IP ללקוחות העובדים תחת מערכות Windows NT וגרסאות קודמות של מערכות הפעלה של Microsoft. באמצעות שיטה זו, משתמשים יכולים לגשת לשרתים לפי שם, במקום להשתמש בכתובות IP שקשה לזהות ולזכור. למשל, שם NetBIOS שניתן במהלך ההתקנה הוא "המחשב של שלום". ה-DNS של אותו מחשב הוא www.nana.co.il ויש למחשב הזה גם כתובת IP **192.25.63.124**. ניתן לגשת למחשב בעזרת כל אחד מהשמות האלה.
	הערה התיקיה Clients שבתקליטור ההתקנה של Windows 2000 Server מכילה שתי תת-תיקיות. התיקיה WIN9X כוללת את לקוח Directory Service ללקוחות Windows 9x. התיקיה WIN9XIPP.CLI מכילה את לקוח Internet Printing עבור חלונות 9x. שירותים אלה מבטלים את דרישת WINS ממחשבי לקוחות Windows 9x.

רכיב אופציונלי	תיאור
שירותים אחרים עבור קבצי רשת ומדפסות	מספק שירותי קבצים והדפסות עבור Macintosh, ושירותי הדפסה עבור Unix.
שירותי התקנה מרחוק	מאפשר להתקין ולהגדיר מחשבי לקוחות חדשים, בלי שיהיה צורך לגשת לכל לקוח. לקוחות היעד חייבים להיות מסוגלים לתמוך באתחול מרחוק. כמו כן תידרש מחיצה נפרדת בשרת עבור שירותי התקנה מרחוק.
אחסון מרוחק	מגדיל את שטח הדיסק על ידי כך שמאפשר גישה נוחה יותר למדיה ניידת, כגון קלטות. שימוש נדיר יותר הוא העברת ואחזור נתונים באופן אוטומטי לקלטת וממנה כנדרש.
Terminal Services (שירות מסופים)	מאפשר הפעלת ישומי לקוחות על השרת כך שמחשבי הלקוחות מתפקדים כמסופים ולא כמערכות עצמאיות. השרת מספק סביבת עבודה Multisession ומפעיל את התוכניות מבוססות-Windows שבהם משתמשים הלקוחות. אם תתקין שירותי מסופים, עליך להתקין גם הרשאות עבור שירותי מסופים (כדי לתת הרשאות ללקוחות שירותי מסופים). אולם, ניתן להנפיק רשיונות זמניים המאפשרים ללקוחות להשתמש בשרתי מסופים ל- 90 יום.
Terminal Services Licensing (שירות הרשאות למסופים)	מאפשר רישום ומעקב אחר רשיונות ללקוחות שירותי מסופים. אם התקנת שירותי מסופים, עליך להתקין גם שירות הרשאות למסופים (כדי לתת הרשאות ללקוחות שירותי מסופים). אולם, ניתן להנפיק רשיונות זמניים המאפשרים ללקוחות להשתמש בשרתי מסופים ל- 90 יום.
Windows Media Services	מספק תמיכה במולטימדיה ומאפשר העברת תוכן (Content) באמצעות Advanced Streaming Format על פני האינטרנט או האינטראנט.

סיכום שיעור

לפני שתתחיל להתקין את Windows 2000 Server, עליך לאסוף את כל החומר הדרוש לך, לוודא שהחומרה שברשותך מסוגלת לתמוך במערכת Windows 2000, ולקבל החלטות על אופן ההתקנה של Windows 2000 Server. לדוגמה, עליך לוודא שהחומרה שלך מתאימה לדרישות הסף של החומרה ולבדוק את כל החומרה לתאימות עם Windows 2000. עליך להחליט כיצד לחלק את הדיסק הקשיח למחיצות, ובאיזו מערכת קבצים תשתמש במחיצה. עליך לבחור סוג הרשאות, באיזו רשת להשתתף, וסוג ההתקנה. כמו כן עליך להחליט אילו רכיבים אופציונליים תרצה להתקין. נקיטת צעדים אלה תכין אותך להתקנה ותמנע בעיות אפשריות.

שיעור 2: התקנת Windows 2000 Server

לאחר שביצעת את הפעולות הנדרשות להכנת ההתקנה של Windows 2000 Server, תוכל להתחיל את תוכנית ההתקנה של Windows 2000. שיעור זה מתמקד בביצוע התקנה חדשה של Windows 2000 Server. הוא מתחיל בדיון על תוכנות ההתקנה השונות ועובר לתיאור שלבי ההתקנה עצמם.

לאחר שיעור זה, תוכל

- לקבוע באיזו תוכנית התקנה להשתמש להתקנת Windows 2000 Server.
- לתאר את שלושת השלבים של הליך ההתקנה.
- לבצע התקנה חדשה של Windows 2000 Server.

זמן לימוד משוער: 30 דקות

תוכניות ההתקנה של Windows 2000 Server

בכל שיטה שתשתמש להתקנת Windows 2000 Server, חובה להפעיל את תוכנית Winnt.exe או Winnt32.exe. תוכל להשתמש בתוכנית Setup.exe לטעינת Winnt.exe או Winnt32.exe, או שתוכל לטעון את Winnt32.exe או Winnt.exe ישירות.

- ❖ להתקנה נקייה על מחשב בו מערכת הפעלה MS-DOS או Windows 3.x, הפעל את Winnt.exe משורת הפקודה של MS-DOS.
- ❖ להתקנה נקייה במערכות Windows 9x או Windows NT Workstation, הפעל את Winnt32.exe.
- ❖ להתקנה נקייה או שדרוג ממערכת Windows NT Server 3.51/4.0, הפעל את Winnt32.exe.

הערה להתקנת שדרוג, ראה שיעור 3 בפרק זה.

ניתן להפעיל מספר מתגים (Switches) עם Winnt.exe ו-Winnt32.exe, כדי להתאים את אופן ההתקנה של Windows 2000 Server במחשב שלך.

תוכנית ההתקנה של Windows 2000

תוכנית ההתקנה של Windows 2000, Setup.exe נמצאת בספריית השורש של תקליטור ההתקנה של Windows 2000 Server. בעת הפעלת Setup.exe, יופיע מסך תקליטור Windows 2000 של Microsoft. משם, תוכל לבצע התקנה של Windows 2000 Server,

להוסיף רכיבים, לדפדף בתקליטור, או לצאת מתוכנית ההתקנה. אם תבחר באפשרות Install Windows 2000, תופעל תוכנית Winnt.exe או Winnt32.exe, בהתאם למערכת ההפעלה הנוכחית שבשימוש. אם אפשרות ההפעלה האוטומטית (Autorun) של תקליטור פעילה במערכת שלך, מסך תקליטור Windows 2000 יופיע בעת הכנסת תקליטור ההתקנה של Windows 2000 Server לכונן התקליטורים. Autorun קורא ל-Setup.exe, הבודק את מערכת ההפעלה. אם תוכנית ההתקנה (Setup) מזהה שהמחשב פועל תחת מערכות הפעלה Windows NT Server 3.51, Windows NT Server 4 או גירסה קודמת של Windows 2000 Server, תתבקש לשדרג או להתקין את Windows 2000. אם מותקנת גירסה חדשה יותר של Windows 2000 Server על המחשב, Setup.exe לא תאפשר המשך התקנת Windows 2000 Server.

הערה ניתן להשתמש בתוכנית Setup.exe אך ורק מתוך מערכת ההפעלה הקיימת, אבל לא מתוך DOS או Windows 3.11.

תוכנית ההתקנה Winnt.exe

ככלל, תוכנית Winnt.exe משמשת להתקנות דרך הרשת כאשר יש ברשת לקוח MS-DOS. Winnt.exe מבצעת את הפעולות הבאות:

1. יוצרת תיקיה זמנית WIN_NT.~BT במחיצת המערכת ומעתיקה קבצי אתחול Setup למחיצה זו.
2. יוצרת תיקיה זמנית WIN_NT.~LS ומעתיקה את קבצי Windows 2000 מהשרת לתיקיה זו.
3. מנחה משתמשים לכבות ולהפעיל מחדש את המערכת. לאחר שהמחשב מתחיל שנית, תפריט האתחול מופיע וההתקנה נמשכת.

Winnt.exe מתקינה את Windows 2000 Server וניתנת להפעלה ממנחה הפקודה (Command Prompt) של MS-DOS או של כל מערכת הפעלה windows, 16 סיביות.

מתגים של Winnt.exe

תוכל להשתמש במתגים (Switches) הבאים להתאמת אפיוני תוכנית ההתקנה Winnt.exe:

WINNT [/s[:sourcepath]] [/t[:tempdrive]] [/u[answer_file]]
[/udf:id[,UDF_file]] [/r:folder] [/rx:folder] [/e:command] [/a]

מתגים אלה מתוארים בפירוט בטבלה הבאה:

מתג	תיאור
/s[:*sourcepath*]	מציין את מיקום קבצי Windows 2000. המיקום חייב להיות נתיב מלא של האיות x:[path] או UNC תקף.

מתג	תיאור
/t[:*tempdrive*]	מורה לתוכנית ההתקנה לשים קבצים זמניים בכונן המצוין ולהתקין את Windows 2000 בכונן זה. אם לא תציין מיקום, התוכנית תנסה לאתר כונן עבורך.
/u[:*answer file*]	מבצע התקנה אוטומטית תוך שימוש ב- Answer File - קובץ תשובות (דורש s/). קובץ התשובות מספק תשובות לחלק או לכל המנחים שאליהם מגיב משתמש הקצה בהתקנה רגילה.
/udf:id[,UDF_*file*]	מציין מזהה (id) שבו משתמשת תוכנית ההתקנה להגדרת ייחודיות קובץ התשובות (ראה u/) תוך שימוש ב- Uniqueness Database File (UDF), קובץ ייחודיות הנתונים). מקדם udf/ דורס ערכים בקובץ התשובות והמזהה קובע אילו ערכים בקובץ UDF ישמשו. אם לא צוין קובץ UDF_file כלשהו, תוכנית ההתקנה תנחה אותך להכניס דיסקט המכיל את קובץ $Unique$.udb.
/r[:*folder*]	מציין תיקיה חליפית להעתקה. התיקיה תישאר לאחר סיום תוכנית ההתקנה.
/rx[:*folder*]	מציין תיקיה חליפית להעתקה. התיקיה תמחק לאחר סיום תוכנית ההתקנה.
/e	מציין פקודה שתבוצע עם סיום תוכנית ההתקנה במצב GUI (GUI-mode).
/a	מאפשר אופציות גישה.

תוכנית ההתקנה Winnt32.exe

Winnt32.exe משמשת להתקנת Windows 2000 Server ממחשב שבו מותקנת מערכת הפעלה Windows 95, Windows 98, או Windows NT. ניתן להפעיל את התוכנית על ידי לחיצה כפולה על Winnt32.exe בשורש של תיקיית המקור (כגון i386\) שבתקליטור ההתקנה של Windows 2000 Server, או בנקודת שיתוף ברשת עבור התקנה דרך הרשת. תוכל גם להפעיל את Winnt32.exe על ידי הפקודה **הפעל** (Run) מתפריט ההתחלה (Start), המאפשרת הגדרת מתגים. בנוסף, הפקודה Winnt32.exe ניתנת להפעלה משורת הפקודה במערכות Windows 95, Windows 98, או Windows NT (כל מערכות ההפעלה 32 סיביות של Windows).

אם יוזמת ההתקנה של Windows 2000 Server נעשית דרך הרשת, Winnt32.exe יוצר תיקיה זמנית WIN_NT.~LS ומעתיק את קבצי Windows 2000 Server מהשרת לתיקיה זו. התיקיה הזמנית נוצרת במחיצה הראשונה שגודלה מספיק, אלא אם מתג t/ ציין אחרת. שלב זה ידוע כשלב לפני-העתקה.

מתגים של Winnt32.exe

תוכל להשתמש במתגים (Switches) הבאים להתאמת אפיוני תוכנית ההתקנה Winnt32.exe :

winnt32 [/s:sourcepath] [/tempdrive:drive_letter]
[/unattend[num]:
[answer_file]] [/copydir:folder_name]
[/copysource: folder_name]
[/cmd:command_line] /debug[level]:[filename]]
[/udf:id[,UDF_file]]
[/syspart:drive_letter] [/checkupgradeonly] [/cmdcons]
[/m:folder_name]
[/makelocalsource] [/noreboot]

מתגים אלה מתוארים בפירוט בטבלה הבאה :

מתג	תיאור
/s:*sourcepath*	מציין את מקום מקור קבצי Windows 2000. להעתקת קבצים ממספר שרתים בו-זמנית, הגדר multiple /s sources (מקורות s/ רבים). אם השתמשת במתגים multiple /s, השרת הראשון שהגדרת חייב להיות זמין, אחרת ההתקנה תיכשל.
/tempdrive:*drive_letter*	מורה לתוכנית ההתקנה לשים קבצים זמניים במחיצה המצוינת ולהתקין את Windows 2000 במחיצה זו.
/Unattend	משדרג את גרסת Windows 2000 הקודמת שלך במצב התקנה אוטומטית. כל הגדרות המשתמש נלקחות מההתקנה הקודמת, כך שלא נדרשת התערבות המשתמש בעת ההתקנה. שימוש במתג unattend/ לביצוע התקנה אוטומטית, מאשרת שקראת והסכמת לתנאי **E**nd-**U**ser - EULA **L**icense **A**greement (הסכם רשיון משתמש קצה) עבור Windows 2000. לפני שימוש במתג זה להתקנת Windows 2000 בארגון אליו אינך משויך, עליך לוודא שמשתמש הקצה קיבל, קרא ואישר את תנאי רשיון EULA של Windows 2000. Original Equipment OEM (Manufacture - יצרני ציוד/מחשבים מקורי), לא יכולים להגדיר מקש זה במחשבים הנמכרים למשתמשי קצה.

מתג	תיאור
/unattend[*num*][*:answer_file*]	מבצע התקנה חדשה במצב התקנה אוטומטית. קובץ התשובות מספק את ההגדרות הייחודיות שלך לתוכנית ההתקנה. Num הוא מספר השניות שחלף מהזמן שתוכנית ההתקנה סיימה להעתיק את הקבצים עד לזמן בו היא מתחילה את המחשב מחדש. תוכל להשתמש ב-num בכל מחשב המפעיל Windows NT או Windows 2000. מציין מקום answer_file הוא שם קובץ התשובות.
/copydir:folder_name	יוצר תיקיה חדשה בתוך התיקיה שבה מותקנים קבצי Windows 2000. לדוגמה, אם תיקיית המקור כוללת תיקיה בשם Private_drivers שבה שינויים המיועדים רק לאתר שלך, תוכל להקליד **copydir:Private_drivers/** כדי שתוכנית ההתקנה תעתיק את התיקיה הזו לתיקיית Windows 2000 המותקנת שלך. במצב זה מיקום התיקיה החדשה יהיה **%Systemroot%\Private_drivers**. תוכל להשתמש במתג copydir/ ליצירת כמה תיקיות נוספות שתרצה.
/copysource:folder_name	יוצר תיקיה חדשה בתיקיה בה מותקנים קבצי Windows 2000. לדוגמה, אם תיקיית המקור כוללת תיקיה בשם Private_drivers, בה שינויים המיועדים רק לאתר שלך, הקלד **copysource:Private_drivers/** כדי שתוכנית ההתקנה תעתיק תיקיה זו לתיקיית Windows 2000 המותקנת שלך, ותשתמש בקבצים שלה בעת ההתקנה. במצב זה מיקום התיקיה הזמנית יהיה - **%Systemroot%\Private_drivers**. שלא כמו התיקיות שיצר מתג copydir/, תיקיות הנוצרות באמצעות הפקודה copysource/ נמחקות לאחר סיום תוכנת ההתקנה.
/cmd:command_line	מורה לתוכנית ההתקנה לבצע פקודה מסוימת לפני שלב ההתקנה הסופי. אירוע זה קורה לאחר שהמחשב אתחל פעמיים ולאחר שתוכנית ההתקנה אספה את כל נתוני התצורה הנדרשים, אך לפני שתוכנית ההתקנה סיימה.
/debug[level][:filename]	יוצר Debug Log (יומן איתור שגיאות) ברמה הנדרשת. לדוגמה, debug4:C:\Win2000.log/. קובץ היומן של ברירת המחדל הוא systemroot%\Winnt32.log%, כאשר רמת Debug הוגדרה 2. רמות log (יומן) הן כדלקמן: **0** - שגיאות חמורות, **1** - שגיאות, **2** - אזהרות, **3** - מידע, **4** - מידע מפורט לתיקון שגיאות. כל רמה כוללת את הרמה שמתחתיה.
/udf:*id*[,UDF_*file*]	מציין מזהה (id) שבו משתמשת תוכנית ההתקנה להגדרת **U**niqueness **D**atabase **F**ile (UDF, קובץ ייחודיות הנתונים), שמשמש לשינוי והתאמת קובץ התשובות (ראה הסבר unattend/). UDF דורס ערכים בקובץ התשובות, והמזהה קובע באיזה ערכים של UDF נעשה שימוש. לדוגמה, udf:RAS_user,Our_company.udb/, ידרוס הגדרות שהוגדרו עבור המזהה RAS_user בקובץ Our_company.udb. אם לא יצוין UDF, תוכנית ההתקנה תנחה את המשתמש להכניס דיסקט המכיל את הקובץ $Unique$.udb.

מתג	תיאור
/syspart:*drive_letter*	מציין שניתן להעתיק קבצי אתחול של תוכנית ההתקנה לדיסק הקשיח, לסמן את הדיסק כפעיל, ואז להתקין את הדיסק במחשב אחר. כאשר תתחיל מחשב זה, הוא יתחיל מייד בשלב הבא של תוכנית ההתקנה. השתמש תמיד במתג tempdrive/ עם מתג syspart/. מתג syspart/ עבור Winnt32.exe פועל רק על מחשב שמותקנת בו מערכת הפעלה Windows NT 3.51, Windows NT 4.0 או Windows 2000. לא ניתן להפעילו ממערכות הפעלה Windows 9x.
/checkupgradeonly	בודק את תאימות השדרוג של המחשב עם Windows 2000. עבור שדרוגים ממערכות Windows 95 או Windows 98, תוכנית ההתקנה יוצרת דוח בשם Upgrade.txt בתיקיית ההתקנה של Windows. לשדרוגים של Windows NT 3.51 או 4.0, הוא שומר את הדוח ליומן Winnt32.log בתיקיית ההתקנה.
/cmdcons	מוסיף אפשרות Recovery Console למסך האפשרויות של מערכת ההפעלה לתיקון התקנה שנכשלה. לשימוש רק לאחר התקנה.
/m:*folder_name*	מגדיר לתוכנית ההתקנה להעתיק קבצים חליפיים מאתר חליפי. מורה לתוכנית ההתקנה לחפש באתר החליפי תחילה, ואם קבצים קיימים, להשתמש בהם במקום בקבצים שבמיקום ברירת המחדל.
/makelocalsource	מורה לתוכנית ההתקנה להעתיק את כל קבצי המקור של ההתקנה לדיסק הקשיח המקומי. השתמש במתג makelocalsorce/ בעת התקנה מתקליטור לאספקת קבצי ההתקנה כאשר התקליטור אינו זמין בהמשך ההתקנה.
/noreboot	מורה לתוכנית ההתקנה שלא לאתחל את המחשב מחדש לאחר ששלב העתקת הקבצים של Winnt32.exe הסתיים כדי שתוכל לתת פקודה נוספת.

הליך ההתקנה

הליך התקנת Windows 2000 Server כולל שלושה שלבים:

1. שלב טרום-העתקה (Pre-Copy Phase),
2. מצב טקסט (Text Mode),
3. מצב ממשק משתמש גרפי (GUI).

Pre-Copy Phase

בשלב טרום-העתקה, כל הקבצים הדרושים להתקנה מועתקים לספריות זמניות על הדיסק הקשיח המקומי. בעת שימוש בפקודות Winnt.exe, Winnt32.exe, ליזום התקנה דרך הרשת, כל הקבצים הדרושים להשלמת ההתקנה מועתקים דרך הרשת לתיקיה

זמנית בשם WIN_NT.~LS. לאחר מכן תוכנית ההתקנה ממשיכה כאילו ההתקנה מתבצעת מהדיסק המקומי, ועוברת למצב טקסט (Text Mode) של הליך ההתקנה ואחר כך לשלב GUI. תוכל לבחור שלא ליצור דיסקטים לאתחול, על ידי סימון בתיבת הסימון Copy All Setup Files From The Setup CD To The Hard Drive. תיבת הסימון נמצאת תחת לחצן Advanced Options. בחירת אפשרות זו יוצרת תיקיה בשם WIN_NT.~BT על הדיסק. תיקיה זו מכילה את הקבצים שהיו אמורים להיות על ארבעת הדיסקטים של האתחול. בעת העתקת הקבצים לתיקיה WIN_NT.~LS - Windows 95, Windows 98 ו-Windows NT עדיין פועלות. עקב כך, זמן Downtime (זמן הדממה/זמן חוסר פעילות) מופחת בעת השדרוג.

Text Mode

בשלב Text Mode, תוכנית ההתקנה מנחה לקבלת נתונים להשלמת ההתקנה. לאחר שאשרת את הסכם הרשיון, הגדר או צור מחיצת התקנה ובחר מערכת קבצים. כל הקבצים הדרושים מועתקים מהתיקיה הזמנית (או התקליטור) לתיקיית ההתקנה או לדיסק הקשיח של מחשב היעד.

הסכם רשיון Windows 2000 Server

הסכם רשיון Windows 2000 Server הוא בן מספר דפים. היעזר במקש Page Down לעלעול בתוך ההסכם, ולחץ F8 לאישורו. ההסכם מופיע לפני Text Mode אם אתה משתמש Winnt32.exe או Autorun להתחלת ההתקנה.

התקנות קיימות

אם תוכנית ההתקנה מאתרת התקנות קיימות כלשהן של Windows 2000, היא תציג אותן ברשימה. תוכל לבחור התקנה קיימת וללחוץ R (Repair) לתיקון התקנה קיימת, או Esc להמשך.

מחיצות

תוכנית ההתקנה מציגה את כל המחיצות הקיימות והשטח הפנוי במערכת. השתמש בחיצים מעלה ומטה כדי לבחור היכן להתקין את Windows 2000 Server. בשלב זה תוכל ליצור ולמחוק מחיצות. הקש Enter להמשך.

מערכות קבצים

תוכנית ההתקנה מאפשרת שמירת מערכת הקבצים הנוכחית בשלמותה או הסבתה ל-NTFS. אם אינך רוצה להסב את המערכת, בחר באפשרות Leave Current File System Intact, שזה מצב ברירת המחדל, והקש Enter להמשך.

תוכנית ההתקנה בודקת את הדיסק הקשיח ומעתיקה את הקבצים הדרושים לך מהתיקיה הזמנית לתיקיית ההתקנה (התיקיה Winnt היא תיקיית ברירת המחדל).

GUI Mode

לאחר השלמת חלק ה- Text Mode של ההתקנה, המחשב מופעל מחדש ומתחיל מצב GUI. מצב זה מאפשר בחירת רכיבים אופציונליים להתקנה ומאפשר בחירת סיסמת ה-administrator.

מצב GUI מורכב משלושה שלבים ברורים:

1. איסוף מידע אודות המחשב שלך.
2. התקנת רשת Windows 2000 Server.
3. השלמת ההתקנה.

איסוף מידע אודות המחשב שלך

שלב איסוף המידע אודות המחשב שלך הוא סדרת תיבות דו-שיח שבהן מערכת Windows 2000 משתמשת לאיסוף מידע על התצורה כדי להגדיר את המערכת. בשלב זה מותקנים אמצעי האבטחה של Windows 2000 וכן מותקנים ומוגדרים התקנים.

הגדרות אזוריות

Windows 2000 מציגה את ההגדרות האזוריות הנוכחיות (ברירת המחדל). תוכל להוסיף תמיכה לשפות נוספות, לשנות את הגדרות האזור שלך עבור המערכת, וגם להגדיר את הגדרות ברירת המחדל של חשבון המשתמש שלך.

הוספת ערכים אישיים לתוכנה

בעת הגדרת המערכת, עליך להכניס את שם הרישום של Windows 2000 Server. בנוסף, תוכל להוסיף את שם החברה שלך, אך אין חובה בכך.

בחירת רשיון הפעלה

עליך לבחור בסוג רשיון הפעלה Per Server (לפי שרת) או Per seat (לפי מושב). אם תבחר לפי שרת, עליך להגדיר את מספר הרשיונות לפי שרת.

שם מחשב וסיסמת מנהל רשת

עליך להכניס שם מחשב (שם NetBIOS של עד 15 תווים) בעת התקנת Windows 2000. שים לב שהשם הניתן אוטומטית הוא בן 15 תווים. השם שתתן חייב להיות שונה משמות מחשבים, קבוצות עבודה או תחומים ברשת. המערכת תציג שם ברירת מחדל עבור המחשב. תוכל לגשת לשם ברירת המחדל או להקליד שם אחר למחשב.

ניתן גם להוסיף סיסמת מנהל (administrator) עבור חשבון המנהל המקומי. סיסמה זו יכולה להיות באורך של עד 127 תווים, או ריקה.

מנהל רכיבים אופציונליים

מנהל הרכיבים האופציונליים מאפשר הוספה או הסרת רכיבים נוספים בעת ואחרי ההתקנה. לפרטים אודות רכיבים אלה, ראה שיעור 1: "הכנות להתקנת Windows 2000 Server".

הגדרות תאריך וזמן

בעת הליך ההתקנה, עליך לבחור את אזור הזמן המתאים ולכוון את התאריך והשעה. אם נדרש, ניתן לכוון חסכון אנרגיה אוטומטי בשעות היום.

התקנת רשת Windows 2000 Server

לאחר שתוכנית ההתקנה משלימה את שלב איסוף הנתונים אודות המחשב שלך, היא חוזרת למסך Windows 2000 Setup. עתה, תוכנית ההתקנה בודקת את המחשב לאיתור מתאמי רשת מותקנים. פעולה זו עשויה להימשך מספר דקות.

הגדרות רשת

התקנת רשת Windows 2000 מתחילה עם תיבת דו-שיח המאפשרת בחירה בין הגדרות רגילות (Typical) לבין הגדרות מותאמות אישית (Custom). התקנה רגילה מגדירה את המערכת עם כל ברירות המחדל: Client for Microsoft Networks, שיתוף בקבצים ומדפסות עבור רשתות Microsoft, ופרוטוקול אינטרנט (TCP/IP) בתצורת לקוח DHCP.

הגדרות מותאמות אישית מאפשרות הגדרת שלושת הפריטים הבאים:

- **Clients** (לקוחות) – לקוח ברירת המחדל הוא Client For Microsoft Networks. תוכל להוסיף שירותי Gateway (ולקוח) עבור Novell NetWare.
- **Services** (שירותים) – שירות ברירת המחדל הוא File and Printer Sharing for Microsoft Networks (שיתוף קבצים ומדפסות ברשתות Microsoft). תוכל להוסיף SAP Agent ו-QoS Packet Scheduler. ניתן לשנות את ההגדרות של File and Printer Sharing for Microsoft Networks על ידי הארת השירות ולחיצה על Properties. פעולה זו תאפשר מיטוב הגדרות שירות השרת ואספקת שירות שרת תואם ללקוחות LAN Manager 2.x .
- **Protocols** (פרוטוקולים) – פרוטוקול ברירת המחדל הוא פרוטוקול אינטרנט (TCP/IP). תוכל להוסיף פרוטוקולים נוספים, כולל NWLink IPX/SPX, NetBEUI, DLC, AppleTalk, Network Monitor Driver ואחרים. ניתן גם לשנות את ההגדרות של פרוטוקול (אם ישים) על ידי הארת הפרוטוקול ולחיצה על Properties.

השלמת ההתקנה

שלב השלמת ההתקנה מבצע את הפעולות הבאות ואינו דורש התערבות המשתמש. הטבלה להלן סוקרת את המטלות המבוצעות על ידי תוכנית ההתקנה בשלב זה.

מטלה	תיאור
העתקת קבצים	תוכנית ההתקנה מעתיקה את כל הקבצים הדרושים שנותרו לספריית ההתקנה, כגון אביזרים ומפות סיביות.
הגדרת המחשב	תוכנית ההתקנה יוצרת את תפריט ההתחלה, קבוצות תוכנה, מגדירה Spooler (תוכנית אוגר ההדפסה ברקע) של המדפסת, את המדפסות, שירותים, חשבון ה-administrator, גופנים, קובץ ההחלפה (Pagefile), ואת רישום ספריות הקישור הדינמיות (DLL - **D**ynamic **L**ink **L**ibraries).
שמירת ההגדרה (תצורה)	תוכנית ההתקנה שומרת את התצורה ב-Registry (רישום המערכת), יוצרת את תיקיית Repair (המכילה את כל נתוני הרישום), ומאפסת את הקובץ Boot.ini.
הסרת קבצים זמניים	תוכנית ההתקנה מסירה את הקבצים הזמניים והספריות שנוצרו ושימשו לצורך ההתקנה, כגון התיקיה WIN_NTS.~LS, וכן גם דוחסת את קבצי Hives (קבצים המכילים נתוני רישום מערכת (Registry).

תרגיל 1 : התקנת Windows 2000 Server

בתרגיל זה, תתקין Windows 2000 Server על מחשב ללא מחיצות מפורמטות. בעת ההתקנה, תשתמש בתוכנית Windows 2000 Server Setup ליצירת מחיצה על הדיסק, בה תתקין את Windows 2000 Server כשרת עצמאי בקבוצת עבודה.

הליך 1 : יצירת דיסקטים של התקנה עבור Windows 2000 Server Setup

בצע הליך זה על מחשב המפעיל MS-DOS או כל גירסה של חלונות שבה יש גישה לתיקיה Bootdisk שבתקליטור ההתקנה של Windows 2000 Server.

אם המחשב שלך בתצורת כונן תקליטורים לאתחול, תוכל להתקין את Windows 2000 ללא הדיסקטים של ההתקנה. להשלמת תרגיל זה כמפורט, יש לבטל תמיכת תקליטור אתחול ב-BIOS.

חשוב הליך זה דורש ארבעה דיסקטים מפורמטים של 1.44MB. אם תשתמש בדיסקטים המכילים נתונים, נתונים אלה יידרסו ללא אזהרה.

---

1. הדבק תוויות כדלקמן על ארבעה דיסקטים מפורמטים 1.44MB :

   דיסקט התקנה Windows 2000 Server מס׳ 1

   דיסקט התקנה Windows 2000 Server מס׳ 2

   דיסקט התקנה Windows 2000 Server מס׳ 3

   דיסקט התקנה Windows 2000 Server מס׳ 4

2. הכנס את תקליטור Windows 2000 Server לכונן התקליטורים.

3. אם מופיעה תיבת הדו-שיח של תקליטור Windows 2000 המנחה אותך להתקין או לשדרג ל-Windows 2000, לחץ Exit.

4. פתח חלון שורת פקודה (Command Prompt).

5. בשורת הפקודה, עבור לכונן התקליטורים שלך. לדוגמה, אם האות המייצגת את כונן התקליטורים שלך היא E, הקלד **:E** והקש Enter.

6. במנחה הפקודה, החלף לתיקיה Bootdisk על ידי הקלדת **cd bootdisk** והקש Enter.

7. אם אתה מכין את דיסקטים אתחול ההתקנה במחשב המפעיל MS-DOS, מערכת הפעלה 16 סיביות של Windows או מערכת הפעלה Windows 9x, הקלד **makeboot a:** (כאשר :A הוא שם כונן הדיסקטים) והקש Enter.

   Windows 2000 תציג הודעה שתוכנה זו יוצרת ארבעה דיסקטים להתקנת Windows 2000. כמו כן תופיע הודעה שנדרשים ארבעה דיסקטים High Density (מפורמטים בצפיפות גבוהה).

8. הקש מקש כלשהו להמשך. Windows 2000 תציג הודעה המנחה אותך להכניס את הדיסקט שיהיה Windows 2000 Setup Boot Disk (דיסקט אתחול ההתקנה של Windows 2000).

9. הכנס את הדיסקט המפורמט הריק עם התווית ***דיסקט התקנה* Windows 2000 Server מס׳ 1** לכונן הדיסקטים, והקש מקש כלשהו להמשך.

   לאחר ש-Windows 2000 תיצור את הדיסקט, היא תציג הודעה המנחה אותך להכניס את הדיסקט עם תווית ***דיסקט התקנה* Windows 2000 Server מס׳ 2**.

10. הוצא את דיסקט מספר 1, הכנס את הדיסקט המפורמט הריק עם התווית ***דיסקט התקנה* Windows 2000 Server מס׳ 2** לכונן הדיסקטים, והקש מקש כלשהו להמשך.

    לאחר ש-Windows 2000 תיצור את הדיסקט, היא תציג הודעה המנחה אותך להכניס את הדיסקט עם תווית ***דיסקט התקנה* Windows 2000 Server מס׳ 3**.

11. הוצא את דיסקט מספר 2, הכנס את הדיסקט עם התווית **דיסקט התקנה Windows 2000 Server מס' 3** לכונן הדיסקטים, והקש מקש כלשהו להמשך. לאחר ש-Windows 2000 תיצור את הדיסקט, היא תציג הודעה המנחה אותך להכניס את הדיסקט עם תווית **דיסקט התקנה Windows 2000 Server מס' 4**.

12. הוצא את דיסקט מספר 3, הכנס את הדיסקט עם התווית **דיסקט התקנה Windows 2000 Server מס' 4** לכונן הדיסקטים, והקש מקש כלשהו להמשך.

    לאחר ש-Windows 2000 תיצור את הדיסקט, היא תציג הודעה שהליך יצירת הדיסקטים הסתיים.

13. בשורת הפקודה, הקלד Exit והקש Enter.

14. הוצא את הדיסקט מכונן הדיסקטים ואת התקליטור מכונן התקליטורים.

הליך 2: הפעלת נוהל לפני-העתקה והגדרת מצב טקסט עבור Windows 2000 Server

יש לבצע הליך זה על Server01. לביצוע הליך זה יוצאים מתוך הנחה שב-Server01 לא מותקנת מערכת הפעלה, אין בדיסק מחיצות ותמיכת אתחול באמצעות תקליטור מבוטלת (אם קיימת). כדי לוודא ש-Server01 מתאים לכל הדרישות המקדימות להתקנה, אנא עיין בהקדמה לספר זה.

1. הכנס את הדיסקט המסומן "דיסקט התקנה Windows 2000 Server מס' 1" לכונן הדיסקטים, הכנס את תקליטור Windows 2000 Server לכונן התקליטורים, וחזור והפעל את Server01.

   לאחר שהמחשב מתחיל, תוכנית ההתקנה של Windows 2000 תציג הודעה קצרה המציינת שתצורת המערכת בבדיקה, ואז יופיע מסך ההתקנה של Windows 2000.

   שים לב שהסרגל האפור בתחתית המסך מעיד שהמחשב בבדיקה ושמערכת Windows 2000 Executive נטענת. זו הגירסה המינימלית של Kernel (ליבת) Windows 2000.

2. כאשר תתבקש על ידי המנחה, הכנס דיסקט התקנה מס' 2 לכונן הדיסקטים והקש Enter. תוכנית ההתקנה מציינת שהיא טוענת את HAL, גופנים, נתונים ייחודים לאזור, מנהלי התקן אפיק ורכיבי תוכנה נוספים לתמיכה בלוח האם, אפיק וחומרה נוספת במחשב שלך. תוכנית ההתקנה טוענת גם את קבצי התוכנה של Windows 2000 Setup.

3. כאשר תתבקש על ידי המנחה, הכנס דיסקט התקנה מס׳ 3 לכונן הדיסקטים והקש Enter. תוכנית ההתקנה מציינת שהיא טוענת את בקרי המנהלים של התקני הכוננים. לאחר טעינת בקרי המנהלים של הכוננים, תוכנית ההתקנה מאתחלת את מנהלי ההתקנים המתאימים לתמיכה בגישה לכוננים. תוכנית ההתקנה עלולה להשתהות מספר פעמים במהלך פעולה זו.

4. כאשר תתבקש על ידי המנחה, הכנס דיסקט התקנה מס׳ 4 לכונן הדיסקטים והקש Enter.

תוכנית ההתקנה טוענת את מנהלי ההתקנים של הציוד ההיקפי, כגון מנהל ההתקן של כונן הדיסקטים ומערכת הקבצים, ואז היא מאתחלת את Windows 2000 Executive וטוענת את שאר תוכנית ההתקנה של Windows 2000.

אם אתה מתקין גרסת הדגמה (Evaluation Copy) של Windows 2000, יופיע מסך הודעות ובו הודעה שאתה עומד להתקין גרסת הדגמה של Windows 2000.

5. קרא את הודעת ההתקנה, והקש Enter להמשך. תוכנית ההתקנה תציג את מסך Welcome To Setup (ברוך הבא להתקנה).

שים לב, שבנוסף להתקנת Windows 2000, תוכל להשתמש בתוכנית ההתקנה של Windows 2000 לתיקון התקנה פגומה של Windows 2000.

6. קרא את הודעת Welcome To Setup והקש Enter להתחלת שלב ההתקנה של Windows 2000 Setup. תוכנית ההתקנה תציג את הסכם הרשיון.

7. קרא את הסכם הרשיון, תוך הקשה על Page Down, כדי לעלעל לתחתית המסך.

8. בחר I Accept The Agreement (אני מקבל את ההסכם) באמצעות F8.

תוכנית ההתקנה תציג את מסך ההתקנה של Windows 2000 Server, ותנחה אותך לבחור אזור פנוי בדיסק, או מחיצה קיימת בה תתקין את Windows 2000. שלב זה בתוכנית ההתקנה הוא אמצעי ליצירה ומחיקת מחיצות בדיסק הקשיח.

אם אין מחיצות ב-Server01 (כנדרש עבור תרגיל זה), תראה שהדיסק המופיע על המסך כולל מחיצה לא מפורמטת.

9. ודא שהמחיצה הלא מחולקת מוארת, והקש C.

תוכנית ההתקנה תציג את מסך ההתקנה של Windows 2000, תאשר שבחרת ליצור מחיצה חדשה באזור שאינו מחולק למחיצות, ותיידע אותך מה הגודל המזערי והמירבי של המחיצה שתוכל ליצור.

10. הגדר את גודל המחיצה שברצונך ליצור (2048MB), והקש Enter להמשך.

הערה אף שתוכל ליצור מחיצות נוספות מהשטח הלא מחולק שנותר בעת ההתקנה, מומלץ שתבצע פעולות חלוקה נוספות לאחר התקנת Windows 2000. לחלוקת דיסקים קשיחים למחיצות לאחר ההתקנה השתמש ב- Snap-In (תוסף התוכנה) Disk Management.

תוכנית ההתקנה תציג את מסך ההתקנה של Windows 2000, ובו המחיצה החדשה C:\New (Unformatted).

11. ודא שהמחיצה החדשה מוארת והקש Enter. המנחה מבקש שתבחר מערכת קבצים עבור המחיצה.

12. השתמש במקשי החיצים לבחירת Format The Partition Using The NTFS File System, והקש Enter.

תוכנית ההתקנה מפרמטת את המחיצה החדשה עם NTFS. לאחר פרמוט המחיצה, תוכנית ההתקנה סורקת את הדיסק לאיתור פגמים פיסיים העלולים לגרום לתוכנית ההתקנה להיכשל, ואז מעתיקה קבצים לדיסק הקשיח. הליך זה יארך מספר דקות.

בסופו של דבר, תוכנית ההתקנה תציג את מסך ההתקנה של Windows 2000 Server. מד התקדמות אדום מבצע ספירה לאחור במשך 15 שניות לפני שתוכנית ההתקנה חוזרת ומפעילה את המחשב.

13. הוצא את דיסקט ההתקנה מהכונן.

חשוב אם המחשב שלך תומך באתחול מכונן התקליטורים ותכונה זו לא בוטלה (Disabled) ב- BIOS, המחשב יאתחל מתקליטור ההתקנה של Windows 2000 Server לאחר שתוכנית ההתקנה של Windows 2000 תתחיל מחדש. כתוצאה מכך תוכנית ההתקנה תתחיל שוב מההחלה. אם דבר זה קורה, הוצא את התקליטור מהכונן, ואתחל את המחשב שנית.

---

14. תוכנית ההתקנה מעתיקה קבצים נוספים, מאתחלת את המחשב שנית וטוענת את אשף Windows 2000 Setup.

הליך 3: שלב הפעלת מצב GUI ואיסוף נתונים של Windows 2000 Server Setup

הליך זה מתחיל את החלק הגרפי של תוכנית ההתקנה על Server01.

1. לחץ Next על מסך אשף ההתקנה Welcome to The Windows 2000 Setup Wizard, להתחלת איסוף נתונים אודות המחשב שלך.

תוכנית ההתקנה מגדירה תיקיית NTFS והרשאות עבור קבצי מערכת ההפעלה, מאתרת את התקני החומרה במחשב, ואז מתקינה ומגדירה מנהלי התקנים לתמיכה בחומרה שאותרה. הליך זה אורך מספר דקות.

2. בדף הגדרות אזוריות, ודא שהגדרות המערכת, הגדרות המשתמש והמקלדת נכונים עבור השפה והאזור שלך, ולחץ Next.

הערה תוכל לשנות את ההגדרות האזוריות לאחר התקנת Windows 2000 בכרטיסיה Regional Options בלוח הבקרה.

תוכנית ההתקנה תציג חלון Personalize Your Software, ותנחה להקלדת שמך ושם הארגון שלך. תוכנית ההתקנה משתמשת בשם הארגון שלך ליצירת שם ברירת מחדל עבור המחשב. יישומים רבים שתתקין בעתיד ישתמשו בנתון זה לרישום מוצריהם וזיהוי מסמכים.

3. בשדה Name הקלד את שמך; בשדה Organization, הקלד את שם הארגון; לחץ Next.

הערה אם מופיע מסך Your Product Key, הקלד את קוד המוצר (Product Key) המסופק על אריזת תקליטור ההתקנה של Windows 2000 Server, **ולחץ** Next.

תוכנית ההתקנה מציגה את מסך Licensing Mode, ומנחה אותך לבחור סוג רשיון. ברירת המחדל הוא רשיון Per Server (לפי שרת). תוכנית ההתקנה מנחה אותך להקליד את מספר הרשאות המשתמשים שרכשת עבור שרת זה.

4. לחץ על לחצן האפשרויות Per Server Number of Concurrent Connections (מספר חיבורים בו-זמניים לשרת זה) והקלד **5** עבור מספר החיבורים הנוכחיים. לחץ Next.

חשוב האפשרויות Per Server והערך **5** עבור מספר הלקוחות האפשריים בו-זמנית, הם ערכים מומלצים המשמשים בתרגיל זה. עליך להשתמש במספר חוקי של חיבורים בו-זמניים, בהתאם לרשיונות שרכשת. תוכל גם לבחור בהגדרה Per-Seat (לפי מושב) במקום Per Server (לפי שרת).

תוכנית ההתקנה תציג את מסך Computer Name And Administrator Password (שם מחשב וסיסמת מנהל (administrator)).

שים לב שתוכנית ההתקנה משתמשת בשם הארגון שלך ליצירת שם מוצע עבור המחשב.

5. בשדה Computer Name הקלד **SERVER01**. Windows 2000 תציג את שם המחשב באותיות גדולות (רישיות) בלי קשר לאופן ההקלדה.

אזהרה להשלמת תרגיל זה, אסור שהמחשב יהיה מחובר לרשת.

בהמשך ספר זה, ההתייחסות תהיה למחשב שרת Server01. אם לא קראת למחשב שלך Server01, בכל מקום שיש התייחסות לשרת Server01, תיאלץ להחליפו בשם השרת שנתת.

6. בשדה Administrator Password ושדה Confirm Password, הקלד **password** (באותיות קטנות) ולחץ Next. בניגוד לשמות משתמש שאינם תלויי-רישיות (Case Insensitive), סיסמאות הן תלויות-רישיות (Case Sensitive). הקלד סיסמאות רק באותיות קטנות.

במהלך ערכת לימוד עצמית זו סיסמת חשבון ה-administrator תהיה password. בסביבת עבודה אמיתית, יש להשתמש בסיסמה מורכבת עבור חשבון ה-administrator (כזו שתהיה קשה לניחוש). Microsoft ממליצה שילוב אותיות גדולות וקטנות, ספרות ותווים מיוחדים (לדוגמה, Lp6*g9).

תוכנית ההתקנה תציג את מסך Windows 2000 Components, ותציין איזה רכיבי מערכת Windows 2000 היא תתקין.

תוכל להתקין רכיבים נוספים לאחר התקנת Windows 2000 באמצעות יישומון Add/Remove Programs בלוח הבקרה. ודא שמותקנים רק רכיבים שנבחרו על ידי ברירת המחדל בעת ההתקנה. בהמשך הלימוד, תתקין רכיבים נוספים.

7. לחץ Next. אם תוכנית ההתקנה איתרה מודם בעת ההתקנה, היא תציג את מסך החיוג של המודם.

8. אם מופיע מסך Modem Dialing Information (מסך נתוני החיוג של המודם), הכנס את קוד החיוג האזורי ולחץ Next. יופיע מסך Date and Time Settings (הגדרת תאריך ושעה).

חשוב שירותי Windows 2000 מבצעים מטלות רבות שהצלחתן מותנית בהגדרת התאריך והשעה של המחשב. ודא בחירה נכונה של אזור הזמן שלך למניעת תקלות עתידיות.

---

9. הכנס את ערכי התאריך, הזמן והגדרת אזור הזמן ולחץ Next. יופיע מסך Network Settings ותוכנית ההתקנה תתקין את רכיבי הרשת.

הליך 4: השלמת שלב התקנת רכיבי הרשת של Windows 2000 Server Setup

הרשת היא חלק אינטגרלי של Windows 2000 Server וניתן לבחור ולהגדיר תצורות רבות עבורה. בהליך זה, מוגדרת תצורת רשת בסיסית. בתרגילים בהמשך, תתקין רכיבי רשת נוספים.

1. במסך Networking System, ודא בחירת Typical Settings, ולחץ Next להתחלת ההתקנה של רכיבי הרשת של Windows.

   הגדרות אלה יתקינו רכיבי רשת המשמשים לגישה ושיתוף במשאבי הרשת ומגדירה את TCP/IP לקבלת כתובת IP אוטומטית משרת DHCP ברשת.

   תוכנית ההתקנה תציג את מסך קבוצת העבודה או מסך התחום, ותנחה אותך להצטרף לאחד משניהם.

2. במסך Workgroup או Domain, ודא שנבחר לחצן אפשרויות No, This Computer Is Not On A Network Or Is On A Network Without A Domain (לא, מחשב זה אינו ברשת או שהוא ברשת ללא תחום), ושם קבוצת העבודה הוא WORKGROUP, ולחץ Next. תוכנית ההתקנה תציג את מסך Installing Components (התקנת רכיבים), תוך שהיא מציגה את המצב בעת ההתקנה והגדרת שאר רכיבי מערכת ההפעלה בהתאם לברירות שהגדרת. פעולה זו אורכת מספר דקות.

   עתה תוכנית ההתקנה תציג את מסך Performing Final Tasks (מבצעת מטלות אחרונות), המראה את המצב בעת סיום העתקת קבצים, יצירת שינויי תצורה ושמירתם ומחיקת קבצים זמניים. מחשבים בעלי תצורה שאינה מעבר לדרישות הסף של החומרה, עלולים לדרוש 30 דקות או יותר להשלמת שלב זה של ההתקנה.

   עתה תוכנית ההתקנה תציג את מסך אשף Completing The Windows Setup.

3. הוצא את תקליטור Windows 2000 Server מכונן התקליטורים, ולחץ Finish.

חשוב אם המחשב שלך תומך באתחול מכונן התקליטורים ותכונה זו לא בוטלה (Disabled) ב- BIOS, המחשב יאתחל מתקליטור ההתקנה של Windows 2000 Server לאחר שתוכנית ההתקנה של Windows 2000 תתחיל מחדש. כתוצאה מכך תוכנית ההתקנה תתחיל שוב מההחלה. אם דבר זה קורה, הוצא את התקליטור מהכונן, ואתחל את המחשב שנית.

Windows 2000 מתחילה שנית ומפעילה את גרסת Windows 2000 Server החדשה שהותקנה.

הליך 5: השלמת שלב התקנת החומרה של Windows 2000 Server Setup

במהלך שלב אחרון זה של ההתקנה, תאותר כל חומרת Plug and Play (הכנס-הפעל) שלא אותרה בשלבים הקודמים של ההתקנה.

1. עם סיום שלב האתחול, הכנס למחשב על ידי הקשה על שילוב המקשים Ctrl+Alt+Delete.
2. בתיבת הדו-שיח Enter Password, בשדה User Name הקלד **Administrator**, ובשדה Password הקלד **password**.
3. לחץ OK. אם Windows 2000 מאתרת חומרה שלא אותרה בעת ההתקנה, יופיע מסך אשף Found New Hardware (נמצאה חומרה חדשה), המעיד כי Windows 2000 מתקינה את מנהלי ההתקן המתאימים.
4. אם מופיע מסך אשף Found New Hardware, ודא שתיבת סימון Restart The Computer When I Finish (אתחל את המחשב כשאסיים) אינה מסומנת ולחץ Finish, לסיום פעולת האשף Found New Hardware.

   Windows 2000 תציג את תיבת הדו-שיח Microsoft Windows 2000 Configure Your Server. מתיבת סימון זו, תוכל להגדיר מיגוון אפשרויות מתקדמות ושירותים.
5. לחץ על לחצן האפשרויות I Will Configure This Server Later (אגדיר שרת זה מאוחר יותר), ולחץ Next.
6. במסך הבא שמופיע, בטל את הסימון מתיבת הסימון Show This Screen At Startup (הצג מסך זה בעת האתחול).
7. סגור את מסך Configure Your Server.

הליך 6: כיוון הגדרות התצוגה

תוכנית ההתקנה בוחרת רזולוציה (הפרדה) התואמת את מתאם המסך שאתרה. תוכל לשנות את הגדרות ברירת המחדל עתה או בכל עת לאחר התקנת Windows 2000.

אזהרה אם אינך יודע את תדר הרענון (Refresh Frequency) הנתמך על ידי המסך שלך בהגדרות לוח הצבעים ושטח המסך שבחרת, אל תשנה את הגדרות ברירת המחדל. הגדרת תדר רענון גבוה מדי עלול להזיק למסך.

1. אם ברצונך לכוון את הגדרות התצוגה כך שייראו יותר צבעים או להגדיל את רמת ההפרדה של המסך, גש ללוח הבקרה ובחר Display (תצוגה). תופיע תיבת דו-שיח המציגה את מאפייני התצוגה.
2. בחר בכרטיסיה Settings, לכיוון שטח המסך והצבעים, ולחץ OK.

תופיע תיבת הודעות Display Properties, המזהירה שההגדרות החדשות שלך ייושמו ושאם לא תגיב לתיבת ההודעות שתופיע לאחר כיוון הגדרות התצוגה, ישוחזרו הגדרות התצוגה המקוריות.

3. לחץ OK. אם הגדרות התצוגה תקפות, תופיע תיבת הודעות Monitor Settings.
4. לחץ Yes לקביעת השינויים. עתה השלמת את התקנת Windows 2000 Server ואתה מחובר לרשת כ-administrator .
5. סגור את לוח הבקרה.

הערה לסגירה מלאה ונכונה של Windows NT Server, לחץ על לחצן Start, בחר Shutdown, ועקוב אחר ההוראות שיופיעו.

סיכום שיעור

להתקנת Windows 2000 Server עליך להפעיל Winnt.exe או Winnt32.exe. Winnt.exe משמשת במחשבים הפועלים תחת מערכות הפעלה MS-DOS או מערכות הפעלה 16 סיביות של Windows. Winnt32.exe משמשת במחשבים הפועלים תחת מערכות הפעלה 32 סיביות של Windows (Windows 9x, Windows NT, או Windows 2000). תוכל להשתמש במספר פרמטרים עם Winnt.exe ו-Winnt32.exe כדי להתאים את התקנת Windows 2000 Server למחשב שלך. ברגע שמופעל אחד מקבצי ההתקנה, מתחילה התקנת Windows 2000 Server. הליך זה כולל שלושה שלבים: שלב הקדם-העתקה, שלב מצב טקסט (Text Mode) ושלב מצב GUI (GUI Mode). בשלב הקדם-העתקה, כל הקבצים הדרושים להתקנה מועתקים לספריות זמניות בדיסק הקשיח המקומי. בשלב Text Mode, תוכנית ההתקנה מנחה את המשתמש לאספקת נתונים הנדרשים להשלמת ההתקנה. שלב GUI Mode מאפשר בחירת רכיבים אופציונליים להתקנה ובחירת סיסמת ה-administrator.

שיעור 3: שדרוג
ל-Windows 2000 Server

הליך שדרוג שרתים קיימים מ-Windows NT Server ל-Windows 2000 Server הוא אוטומטי בעיקרו. בעת העדכון, תכנית ההתקנה של Windows 2000 מעבירה את הגדרות מערכת ההפעלה הנוכחית ודורשת אך מעט סיוע מהמתקין. שיעור זה יתמקד בשלושה נושאים של הליך השדרוג: שדרוג למערכת הפעלה Windows 2000 Server, שדרוג Windows NT Domains, מיזוג domains.

לאחר שיעור זה, תוכל

- לשדרג מחשב Windows NT לשרת Windows 2000 Server.

זמן לימוד משוער: 30 דקות

שדרוג ל-Windows 2000 Server

שדרוג Member Server כרוך בהליך בסיסי אחד בלבד. לאחר שתתחיל את הליך השדרוג, אשף ההתקנה ידריך אותך בשדרוג. בעת קבלת הנחיה, בחר באפשרות Upgrade To Windows 2000. במהלך השלבים האחרונים של השדרוג, תאסוף תוכנית ההתקנה של Windows 2000 Server נתונים, תוך שימוש בהגדרות הקיימות ממערכת ההפעלה הקודמת.

קיימות מספר סיבות לבחור שדרוג, אם מערכת ההפעלה הקודמת שלך היא מגירסה הניתנת לשדרוג. הגדרת התצורה פשוטה יותר; המשתמשים הנוכחיים, ההגדרות, הקבוצות, הזכויות וההרשאות נשמרים. בנוסף, אין צורך להעתיק קבצים ויישומים בחזרה לדיסק לאחר ההתקנה (אולם, כמו בכל שינוי גדול לדיסק, עליך לגבות את הדיסק לפני ביצוע השדרוג).

אם ברצונך לשדרג ולהשתמש באותם יישומים כבעבר, עיין בקובץ HCL של Windows 2000 באתר http://www.microsoft.com, וקרא את הקובץ Read1st.txt וקובץ Relnotes.doc שבספריית השורש בתקליטור ההתקנה של Windows 2000 Server. תוכל גם להתקין את כלי התמיכה של Windows 2000, הנמצאים בתיקיה \Support\Tools בתקליטור ההתקנה של Windows 2000 Server. כלי התמיכה כוללים את Windows 2000 Server Resource Kit Deployment Planning Guide, עיין בפרק "Testing Applications for Compatibility with Microsoft Windows 2000" שב- Resource Kit.

בעת ביצוע השדרוג, עליך לשקול אם להסב מחיצות FAT16 או FAT32 כלשהן הקיימות במערכת למערכת קבצים NTFS. ניתן להתקין את Windows 2000 Server ולאפשר למחשב להפעיל לעיתים מערכת הפעלה אחרת על ידי הגדרת המחשב כמערכת בעלת אתחול כפול. אולם, שימוש באתחול כפול יוצר מורכבות בנושאי מערכות קבצים.

שדרוג שרתים

Windows 2000 Server תומכת בשדרוג מ-Windows NT 3.51 Server, Windows NT 4.0 Server, וגרסאות קודמות של Windows 2000 Server. אם המחשב מפעיל גרסת Windows NT ישנה יותר מ- Windows NT 3.51, שדרג ל-Windows NT Server 4.0 לפני שדרוג ל-Windows 2000 Server.

הערה Windows 2000 תומכת בכל חבילות השירות (Service Packs) עבור Windows NT 3.51 ו-Windows NT 4.0. שדרוג יישומים קיימים משתנה בהתאם למערכת.

שיטות שדרוג

הדרך הקלה ביותר לשדרג Windows NT Server היא להכניס את תקליטור ההתקנה Windows 2000 Server לכונן התקליטורים. ההפעלה האוטומטית של התקליטור תגרום להפעלת תוכנית Setup.exe שבתקליטור. תוכל גם להפעיל את Winnt32.exe מהתקליטור.

תוכנית ההתקנה אינה יכולה לשדרג את מערכת ההפעלה מהדיסקטים של האתחול או על ידי אתחול מהתקליטור. יש להשתמש ב-Winnt32.exe או Autorun לשדרג את Windows NT Server. כמו כן, תוכל לשדרג את המערכת על ידי הפעלת Winnt32.exe דרך הרשת.

איתור התקנות Windows NT לשדרוג

לאיתור התקנות Windows NT Server במערכת, קובץ C:\Boot.ini נבדק במערכות מבוססות מעבד x86.

הערה Windows 2000 אינה תומכת במערכות מבוססות מעבדי RISC.

מנגנון השדרוג מנסה לגשת למחיצה המצוינת על ידי נתיב **A**dvanced **R**ISC **C**omputing (ARC) בנתיב **<active partition>:\Boot.ini** עבור כל התקנה שהוא מאתר. המחיצה הפעילה היא לרוב :C כך שהפניות לכונן בו הקובץ Boot.ini תהיינה ל-:C. אם תוכנית ההתקנה מצליחה לגשת למחיצה, היא בוחנת את ספריית השורש כדי לאתר את הפריטים הבאים :

- **Directories** (ספריות) – מנגנון ההתקנה מחפש תת-תיקיות System32, System32\Drivers, ו-System32\Config.
- **Files** (קבצים) – מנגנון ההתקנה מחפש את הקבצים Ntoskrnl.exe ו-Ntdll.dll תחת תת-הספריות של System32.

לאחר חיפוש אחר ספריות וקבצים, הליך ההתקנה מנסה לטעון חלקים מרישום המערכת (Registry), כדי לוודא אם נעשה בעבר ניסיון שנכשל לשדרג התקנה זו. תוכנית ההתקנה גם קובעת את סוג התקנת Windows NT הנוכחית, ומוצאת את

המהדורה (שרת או קבוצת עבודה), מספר הגירסה של Windows NT (3.1, 3.5, 3.51, או 4.0), ומספר בנייה (Build).

מספר גרסת המערכת הנוכחית ומספר הבנייה חייבים להיות קטן או שווה למספר הגירסה אליה מתבצע השדרוג. כמו כן המהדורה צריכה להיות Server. מכאן, שהליך שדרוג Windows 2000 Server יכול לשדרג רק מערכות Windows NT Server 3.51 ו-Windows NT Server 4.0.

לאחר שכל ההתקנות שבקובץ C:\Boot.ini אותרו וכל נתון התאים לקריטריונים המפורטים מעלה, תוכנית ההתקנה תציג תפריט ובו רשימת ההתקנות שניתן לשדרג.

אם התקנת שרת Windows NT Server אינה מופיעה ברשימת ההתקנות הניתנות לשדרוג, כנראה שלא תאם את אחת הבדיקות שפורטו מעלה. בשלב זה ניתן להקיש על F3, ליציאה מהשדרוג, ועדיין לאתחל לגרסת Windows NT הנוכחית, כדי לוודא שהיא תואמת את הקריטריונים.

הערה אם קיימים מספר מציינים בקובץ C:\Boot.ini המצביעים על אותה התקנה של Windows NT, התקנה זו מצוינת ברשימת ההתקנות רק פעם אחת.

שדרוג Windows NT Domain

מטלה קריטית בשדרוג הרשת ל-Windows 2000 Server היא שדרוג Windows NT Domain Server. Domains הם תכונה חשובה של Windows NT Server ו-Windows 2000 Server. domain הוא קיבוץ של חשבונות ומשאבי רשת תחת שם domain אחד וגבולות אבטחה משותפים. נדרש domain אחד או יותר אם ברצונך להשתמש בחשבונות משתמשים מבוססי-Domains ותכונות אבטחה של Domains קיימים ב-Windows 2000 Server (דבר זה היה נכון גם לגבי Windows NT Server).

במערכות Windows 2000, שרתים יכולים לשמש באחד משלושת התפקידים הבאים:

1. **D**omain **C**ontroller - DC, המכילים העתקים זהים של חשבונות משתמשים ונתוני מכלול Active Directory Services אחרים בכל תחום נתון;
2. Member Server השייכים לתחום אך אינם כוללים העתקי נתונים של Active Directory Services;
3. Stand-alone Server שאינם שייכים לתחום אלא שייכים לקבוצת עבודה.

חייב להיות לפחות Domain Controller אחד לכל Domain, וככלל, צריכים להיות מספר Domain Controllers, אשר כל אחד מגבה את חשבונות המשתמשים ונתונים אחרים של Active Directory Services עבור האחרים ועוזר באספקת תמיכת התחברות למשתמשים.

עליך לתכנן את תפקידי השרתים ב-Domains של Windows 2000 לפני הפעלת ההתקנה; אולם, ניתן לשנות תפקידים אלה לאחר ההתקנה.

קיימות מספר נקודות חשובות לזכור אודות שדרוג Windows NT Domain קיים ל-Windows 2000 Domain:

- חובה להשתמש במערכת קבצים NTFS ב-Domain Controllers.
- שרתים בהם מחיצות המפורמטות FAT16 או FAT32 יהיו חסרי אבטחה מקומית. במחיצות FAT16 או FAT32, ניתן להגן על תיקיות משותפות רק עם הרשאות שהוגדרו בספריות, לא על קבצים בודדים, ואין הגנה נגד גישה מקומית למחיצות.
- בעת שדרוג Domain Controllers ב- Windows NT Domain ל- Windows 2000, עליך לשדרג את ה-PDC תחילה.

תפקידי השרתים ב-Domains הם בעלי שמות שונים במקצת ב-Windows 2000 Server לעומת Windows NT Server. במערכת Windows NT Server, התפקידים האפשריים היו PDC (**P**rimary **D**omain **C**ontroller), בקר ראשי לתחום - יכול להיות אחד כזה בתחום נתון), BDC (**B**ackup **D**omain **C**ontroller), בקר גיבוי לתחום), שרת חבר (Member Server) או שרת עצמאי (Stand-Alone Server). למערכת Windows 2000 יש רק סוג אחד של Domain Controller (ללא ייעוד "ראשי" או "גיבויי") הכולל גם את תפקידי השרת-חבר והשרת העצמאי. הטבלה להלן מתארת כיצד תוכנית ההתקנה של Windows 2000 מקצה תפקידי שרת בעת השדרוג:

תפקיד בתחום Windows NT	**תפקיד בתחום Windows 2000**
PDC	DC
BDC	בחירה שלך אם DC **או** Member Server
Member Server	בחירה שלך אם Member Server **או** Stand-Alone Server
Stand-Alone Server	בחירה שלך אם Member Server (**אם קיים תחום** Windows 2000 Domain) **או** Stand-Alone Server

שדרוג תחום Windows NT כרוך במספר שלבים:

1. תכנון שדרוג Windows NT Domain.
2. הכנות לשדרוג Windows NT Domain.
3. שדרוג PDC.
4. שדרוג BDC.
5. שדרוג Member Servers.

תכנון שדרוג Windows NT Domain

הנושאים העיקריים שיש לשקול כחלק מתוכנית שדרוג Windows 2000 הם כדלקמן :

❖ **DNS Domain Name Organization** (ארגון שמות תחומי DNS) – פיתוח מבנה ארגוני של שמות Domain עבור Domain השורש של עץ ארגוני, או עצים רבים ביער בעלי שמות Domain לא מקושרים. לאחר ש-Root Domain נוצר ונרשם ב- DNS, ניתן להוסיף child-Domains נוספים לבניית העץ. לדוגמה, microsoft.com הוא Root Domain (שורש) ו-dev.microsoft.com ו-mktg.microsoft.com הם תת-Domains (child-domains).

❖ **Name space organization within large account domains** (ארגון טווח שמות בתחומים עם חשבונות גדולים) – קבע כיצד להשתמש ב-OU (יחידות ארגוניות) לארגן את האנשים ולספק משאבים.

❖ **Domain consolidation** (איחוד Domains) – אזן מחדש ניהול ושליטה של רשתות בעלות ניהול מרכזי ושירותי רשתות מבוזרות, על ידי איחוד משאבי Domains למספר מצומצם יותר של Windows 2000 Domains.

הערה במערכת Windows NT 4 היתה מגבלה ל-40,000 אובייקטים (חשבונות משתמש, קבוצה ומחשבים) ל-Domain. במערכת Windows 2000 ה-Domain מוגבל לסדר גודל של מיליוני אובייקטים. ולכן, בעת שדרוג אין צורך במספר Resource Domains, אלא אחד שכזה - מספיק.

❖ **New machine accounts added for long term organization** (הוספת חשבונות חדשים עבור מחשבים לארגון רחוק-טווח) – קבע את מיקום חשבונות המחשבים ב-OU (יחידות ארגוניות) של Windows 2000. זה הוא חלק חשוב ביישום מדיניות האבטחה של מחשבי Windows 2000.

❖ **Deployment of advanced technologies** (יישום של טכנולוגיות מתקדמות) – יישם טכנולוגיות מתקדמות חדשות כגון אבטחת PKI להתחברות באמצעות כרטיסים חכמים ואימות גישה מרחוק, או אבטחת IP עבור תקשורת נתונים מאובטחת בתקשורת אינטראנט פרטית ואינטרנט ציבורית.

הערה למידע נוסף, עיין ב- "Windows 2000 Support Tools' Deployment and Planning Guide" (כלי תמיכה ותכנון ביזור Windows 2000). תוכנית ההתקנה עבור מדריך זה וכלי תמיכה אחרים ממוקמים בתיקיה \support\tools בתקליטור ההתקנה של Windows 2000 Server.

הכנות לשדרוג Windows NT Domain

גבה את הדיסקים הקשיחים בעת ביצוע שינויים מהותיים בתכולת הדיסקים הקשיחים בשרתים שלך, לפני שתשדרג אותם. לפני השדרוג, כדאי לשקול ניתוק כבל הרשת מה-BDC ברשת Windows NT הקיימת. לאחר שדרוג ה-PDC ל-Windows 2000 Server, ניתן לקדם מערכת מנותקת זו לתצורת Windows NT PDC,

אם נדרש (במהלך שדרוג חסר אירועים מיוחדים, לא היית מקדם את Windows NT BDC ל- PDC, אלא היית ממשיך את הליך השדרוג, ובסופו של דבר חוזר ומחבר את השרת המנותק ומשדרג אותו).

בנוסף, עבור כל מחשב המיועד להיות Domain Controller ב-Windows 2000 Domain, ודא שיש מקום פנוי רב על הדיסק, מעבר לשטח הנדרש על ידי מערכת ההפעלה עצמה. כאשר בסיס הנתונים של חשבונות משתמשים משודרג לתצורת Windows 2000 Server, הוא עשוי להתרחב במידה משמעותית.

הכנות לשדרוג Domain Controller

לפני שדרוג Domain Controller יש לבצע מספר מטלות :

- בטל WINS על ידי שימוש באפשרות Services בלוח הבקרה של Windows NT Server 4.0, כך שבסיס הנתונים של WINS יוכל לעבור הסבה במהלך השדרוג.
- בטל (Disable) DHCP על ידי שימוש באפשרות Services בלוח הבקרה של Windows NT Server 4.0 כדי שניתן יהיה להסב את מסד הנתונים DHCP במהלך השדרוג.
- הכן סביבת בדיקה על ידי יצירת חשבונות משתמשים לבדיקה כדי שתוכל לבחון את השדרוג לאחר סיומו. צור משתמשים וקבוצות התואמים את יישום Windows NT Server 4.0 הנוכחי.

הטבלה להלן מתארת פריטים שאולי תרצה לכלול בסביבת בדיקה, והנחיות ליישומם :

פריט	אופן היישום
מדיניות משתמש וקבוצה	כלול מדיניות משתמש ומדיניות קבוצה שקל לבדוק אותן לאחר השדרוג. לדוגמה, הסרת פקודת Run מתפריט Start.
פרופיל משתמש	הגדר פרופיל משתמשים עבור משתמשי הבדיקה כך שיהיו ברורים וקלים לבדיקה, כגון טפטים שונים לרקעים.
Logon Script (תסריט התחברות)	השתמש בהוראות התחברות קלות לבדיקה לאחר השדרוג, כגון מיפוי כונני רשת באמצעות פקודת Net Use.

הערה רצוי תמיד לבחון שדרוג בסביבה מעבדתית לפני יישומה בסביבת עבודה. לצורך כך, תוכל להסיר BDC מהרשת ולקדמו ל-PDC ברשת פרטית. עתה תוכל לשדרג את ה-PDC ל-Windows 2000 Server. אם הליך זה עבר בהצלחה, תוכל להחזיר מחשב זה לסביבת עבודה.

שדרוג PDC

ה-Domain Controller הראשון שיש לשדרג ב-Windows NT Domain חייב להיות PDC) **P**rimary **D**omain **C**ontroller, בקר התחום הראשי). בעת שדרוג שרת זה תוכל לבחור אם ליצור Domain בעץ חדש או Child Domain בעץ קיים, וכן לבחור אם ליצור יער (Forest) חדש או עץ (Tree) ביער קיים. לשדרוג Domain של שלושה עד חמישה שרתים, צור Domain חדש או יער חדש. בנוסף, עליך להגדיר DNS (Domain Name Space) לקביעת טווח שמות ברמה עליונה עבור הארגון. ניתן להוסיף Domains אחרים לעץ בצורת Child Domains.

בעת השדרוג ניתנת לך האפשרות לבחור מיקום שלושה קבצים חשובים:

1. מסד הנתונים הכולל חשבונות משתמש ונתוני Active Directory נוספים,
2. קובץ Log (יומן),
3. SYSVOL - System Volume File.

ניתן להתקין את מסד הנתונים וקובץ היומן בכל סוג של מחיצה (FAT16, FAT32, או NTFS); מסד הנתונים SAM עלול להתרחב משמעותית מעבר למימדים שהיו לו במערכת Windows NT Server, כך שנדרש לאפשר לו מרחב רב. (בתחילה, קבצי היומן יצרכו שטח קטן מאוד). SYSVOL - System Volume File חייב להיות במחיצת NTFS.

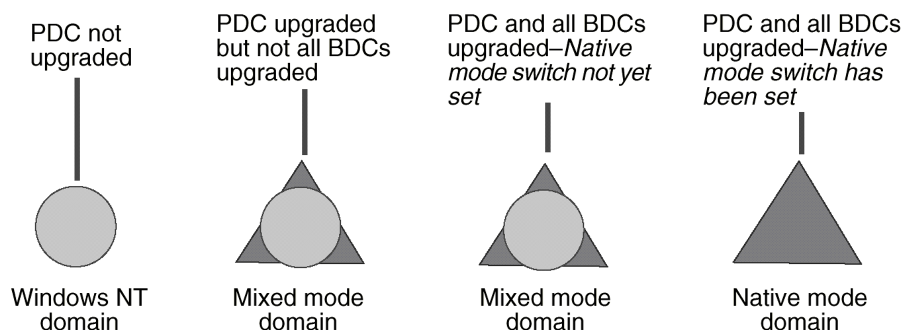
לאחר שהשרת הראשון שודרג ל-Windows 2000 Domain Controller, הוא יהיה תואם לאחור לחלוטין. המשמעות היא שבסביבה רבת-שרתים DC מוצג כ-Windows 2000 DC לשרתי Windows 2000 Servers ולקוחות, אך מדמה PDC של Windows NT 4.0 לשרתים ולקוחות אחרים.

שדרוג BDC

לאחר שדרוג ה-PDC ובחינת פעולתו התקינה, שדרג את כל ה-BDC (**B**ackup **D**omain **C**ontroller). אם ניתן, רצוי להתחיל בשדרוגים מהר ולא להתעכב. ודא שהשרת הראשון ששודרג (שהיה בעבר PDC) פועל וזמין ברשת, בעודך משדרג Domain Controllers אחרים. שרת זה משמש כתבנית עבור Domain Controllers האחרים, להעתקה בעודם משודרגים.

שדרג כל BDC בנפרד, ודא גיבוי כל אחד לפני השדרוג. הפעל ובחן כל שרת ברשת כדי לוודא שהוא פועל כנדרש לפני שדרוג BDC נוסף.

לאחר ששדרגת את כל השרתים ל-Windows 2000 Domain Controllers, ניתנת לך האפשרות לשנות את ה-Domain ממצב מעורב (Mixed Mode) - בו Windows NT Domain Controllers יכולים להתקיים, למצב טהור (Native Mode) - בו רק Windows 2000 Domain Controllers יכולים להתקיים. זוהי החלטה חשובה, כיון שלא תוכל לחזור למצב מעורב לאחר שינוי למצב טהור. תרשים 2.2 מתאר את המעבר מ- Windows NT Domain ל-domain טהור של Windows 2000.



תרשים 2.2 מעבר מ-Windows NT Domain ל- Native Mode Domain של Windows 2000.

Mixed Mode

מצב מעורב מתייחס ל-Domains בהם קיימים גם Windows 2000 Domain Controllers יחד עם Domain Controllers מסוג Windows NT 3.51/4.0. במצב מעורב, PDC משודרג ל-Windows 2000 Server ו-BDC אחד או יותר נשארים כגירסה של Windows NT Server 3.51/4.0. Windows 2000 Domain Controller שהיה PDC משמש ב-Active Directory store לשמירת אובייקטים. הוא עדיין תואם-לאחור לחלוטין, כיון שהוא חושף את הנתונים כמחסן שטוח (Flat Store) למחשבים ברמה נמוכה יותר.

PDC מופיע כ-Windows 2000 Domaoin Controller למחשבי Windows 2000 אחרים, וכ-Windows NT 3.51/4.0 Domain Controller למחשבים שלא שודרגו עדיין.

ב-PDC של Windows 2000, ה-Domain משתמש עדיין בשכפול Master (אב טיפוס) יחיד; הוא מוכר כ-Primary Domain על ידי BDC של Windows NT Server 3.51/4.0. במצב מעורב ה-Domain מוגבל על ידי תפקודיות ה-DCs של Windows NT 4.0. חלק מההגבלות החלות על מערכת Windows 2000 הפועלת במצב מעורב הן:

❖ לא ניתן לעשות Group Nesting (קינון קבוצה).

❖ לקוחות שאינם Windows 2000 אינם יכולים ליהנות מ-Transitive Trust (יחסי אמון משורשרים); הם מוגבלים ליחסי האמון שהיו קודם להתקנת Windows 2000 לצורך קבלת גישה למשאבים (Resources).

Mixed Mode הוא מצב ברירת המחדל והוא לרוב מהווה שלב ביניים ביישום Windows 2000.

Native Mode

לאחר שכל ה-Domain Controllers ב-Domain שודרגו, ניתן לשנות את ה-Domain מ- Mixed Mode ל- Native Mode (ב- Native Mode - כל ה-DCs הם Windows 2000). במצב זה כל הלקוחות משתמשים ב- Transitive Trust (יחסי אמון משורשרים) של Windows 2000. המשמעות היא שמשתמש יכול להתחבר לכל משאב בארגון. Native Mode מאפשר גם קינון קבוצה.

הערה מעבר ל- Native Mode הוא חד-סטרי. לא ניתן להחזיר את ה-Domain ל- Mixed Mode מ- Native Mode.

שדרוג Member Servers

שדרג את ה-Member Servers (שרתים-חברים). ניתן לשדרג שרתים-חברים בכל סדר שהוא.

Domain Consolidation

איחוד תחומים (Domain Consolidation) הוא הליך תכנוני לארגון משאבי Domains כדי לנצל תכונות מתקדמות חדשות של מכלול Active Directory Services במערכת Windows 2000. שינוי תצורת תחומים הוא אפשרות; הוא אינו דרישה ליישום Windows 2000. ניתן לבצע שינוי תצורת Domains במשך הזמן, בעת שדרוג מחשבים בודדים והזזתם ל-Domains שונים. כמו כן, שינוי תצורה הוא פעולה אינטנסיבית האורכת זמן רב, כיון שמעבירים מחשבים ל-Domains חדשים ובקרת גישה מעודכנת ונבדקת כנדרש.

Account Domain - זהו Domain ראשי בו ישמרו כל חשבונות המשתמשים וגם כל ההרשאות שלהם.

Resource Domain - זהו Domain המכיל משאבי רשת (מדפסת וכו') אבל אינו מכיל את חשבונות המשתמשים ברשת. Domain זה מתחבר על ידי יחסי אמון ל-Domain Accounts וממנו מקבל את שמות המשתמשים.

קיימות שתי דרכים כלליות לאחד Domains:

- העברת חשבונות משתמשים מ-Domain אחד לשני, ליצירת Domain אחד גדול יותר.
- העברת שרתים מ-Resource Domain אחד ל-OU של Domain אחר.

הערה ברשת Windows NT משתמשים ב-Resource Domain ו-Account Domain כדי להפוך את ניהול המשתמשים לקל יותר. כך, שאם לחברה יש מספר סניפים ברחבי הארץ, ה-Domain של הסניף הראשי יהיה Domain account (שם ישב מנהל הרשת) ושאר הסניפים יהיו Domain resources ויקבלו את שמות המשתמשים המחשב שבסניף הראשי.

יתרון אחד של Domain Consolidation הוא שניתן להפחית את מספר Master Account Domains, כיון שניתן להרחיב כל Domain כך שיטפל במספר הרבה יותר גדול של חשבונות משתמשים, קבוצות ומחשבים. חיבור Master account domains עשוי להפחית את מספר השרתים ו-Trust Accounts (חשבונות אמון) בין-Domains. אולם, העברת משתמשים מ-Domain אחד לשני, דורשת יצירת סיסמה זמנית חדשה עבור חשבון המשתמש ב-Domain החדש. סיסמאות משתמשים אינן נשמרות כאשר חשבון משתמש מועבר מ-Domain אחד לשני, אף שמזהה האבטחה (**S**ecurity **ID** - SID) עבור המשתמש כן נשמר.

יתרון נוסף של Domain Consolidation הוא שמספר Resource Domains ניתן להפחתה על ידי העברת שרתים מ-Domains קטנים רבים ל-Combined resource domain. ה-Domain Controllers של Domains Resource הופכים ל-Member servers ב-Domain המשולב הגדול. בכך מופחתים מספר יחסי האמון שבין Resource domains ל-Account Domains, ונחסכים משאבי מערכת ב-Domain Controllers. Domain Consolidation מקל על העברת מחשבים מפרויקט אחד לשני, או ממחלקה אחת לשנייה.

Windows 2000 כוללת את התכונות הבאות שמאפשרות שינוי תצורת תחומים :

- ניתן להעביר משתמשים וקבוצות מעבר לגבולות Domains ולשמור על זיהוי האבטחה. היסטוריית מזהה האבטחה נשמרת בחשבון המשתמש, ואסימוני גישה ישמרו את ה-SID הישן והחדש, כדי לשמור על זכויות גישה.
- ניתן להוריד רמה של Domain Controller, להפכו לשרת חבר ואז להעבירו ל-Domain אחר (דבר שלא היה אפשרי ב-Windows NT 4).
- ניתן להגדיר מדיניות אבטחה מרכזית וליישמה במערכות רבות. מדיניות זו יכולה לגדול עם הזמן ולהשתנות. היא משמשת להחלת טכנולוגיות חדשות, כגון אבטחת Public Key (מפתח ציבורי) ואבטחת IP. כאשר מחשבים חדשים מצטרפים ל-Domain, הם מקבלים את מדיניות האבטחה הקיימת ב-Domain באופן אוטומטי.
- ניתן להעביר מחשבים ל-Domains שונים באמצעות כלי ניהול מרחוק.
- ניתן לעדכן זכויות גישה כך שישקפו שינויי מדיניות או שינוי מבנה הארגון.

סיכום שיעור

שדרוג ממערכת Windows NT Server למערכת Windows 2000 Server הוא הליך אוטומטי בעיקרו. הדרך הקלה ביותר לשדרוג Windows NT Server היא להכניס את תקליטור ההתקנה של Windows 2000 לכונן התקליטורים של המחשב. אשף ההתקנה ידריך אותך דרך השדרוג. אולם, נושא חשוב בשדרוג ל-Windows 2000 הוא שדרוג ה-Domain, הכרוך במספר שלבים. תחילה, עליך לתכנן כיצד תשדרג את ה-Domain, כולל הגדרת ארגון שמות Domains ויישום טכנולוגיות חדשות. עתה עליך להתכונן לשדרוג על ידי השלמת מטלות כגון גיבוי קבצים וניתוק כבלי רשת. בנוסף, עליך להתכונן לשדרוג Domain Controllers. השלב הבא בשדרוג התחום הוא שדרוג PDC. לאחר מכן יש לשדרג את ה-BDC ושרתים חברים. לאחר השלמת פעולות אלה, עליך לשקול Domain Consolidation כדי לנצל את התכונות המתקדמות החדשות של מכלול Active Directory Services של Windows 2000.

שיעור 4: איתור תקלות בהתקנת Windows 2000 Server

התקנת Windows 2000 Server אמורה לפעול עד הסיום ללא תקלות כלשהן. אולם, שיעור זה דן בכמה נושאים נפוצים בהם אולי תיתקל בעת ההתקנה.

לאחר שיעור זה, תוכל

- לאתר תקלות בהתקנות Windows 2000.

זמן לימוד משוער: 15 דקות

איתור תקלות במערכת Windows 2000 Server

בעת התקנת Windows 2000 Server אתה עלול להיתקל בבעיות הנובעות, לדוגמה, ממדיה פגומה או חומרה לא מתאימה. הטבלה להלן מפרטת חלק מבעיות ההתקנה הנפוצות ומספקת פתרונות לתיקונם.

תקלה	פתרון
שגיאות מדיה	אם ההתקנה היא מתקליטור, השתמש בכונן תקליטורים אחר. אם אתה עדיין מקבל שגיאות מדיה, בקש תקליטור חליפי על ידי התקשרות ל- Microsoft או לסוכן ממנו רכשת את מערכת ההפעלה.
כונן תקליטורים ללא תמיכה	החלף את כונן התקליטורים בכונן שיש לו תמיכה, או אם לא ניתן, נסה שיטת התקנה אחרת, כגון התקנה דרך הרשת. לאחר השלמת ההתקנה, תוכל להוסיף את מנהל ההתקנים עבור כונן התקליטורים, אם הוא זמין.
חסר מקום על הדיסק	• השתמש בתוכנית ההתקנה ליצירת מחיצה משטח פנוי על הדיסק הקשיח. • מחק וצור מחיצות כנדרש ליצירת מחיצה גדולה דיה עבור ההתקנה. • חזור ופרמט מחיצה קיימת להגדלת המקום.

תקלה	פתרון
כשל בהפעלת שירות תלוי (Dependency Service)	השתמש באשף ההתקנה של Windows 2000, וחזור לתיבת הדו-שיח Network Settings, ודא שהתקנת את הפרוטוקול הנכון ומתאם הרשת. ודא שלמתאם הרשת יש את הגדרות התצורה הנכונות, כגון סוג Transceiver (מתאם יציאת כבל בכרטיס בעל יציאות שונות) וששם המחשב המקומי הוא ייחודי ברשת.
אין אפשרות להתחבר ל-DC	• ודא ששם ה-Domain נכון. • ודא שהשרת המפעיל את שירות DNS ו-DC מקוונים. אם אינך מצליח לאתר Domain Controller, התקן לתוך קבוצת עבודה והצטרף ל-Domain לאחר ההתקנה. • ודא שכרטיס מתאם הרשת והגדרות הפרוטוקול נכונים. • אם אתה מתקין את Windows 2000 שנית ומשתמש באותו שם מחשב, מחק וצור שנית את חשבון המחשב.
לא ניתן להתקין או להתחיל את Windows 2000 Server	ודא ש-Windows 2000 מאתרת את כל החומרה ושכל החומרה תואמת את רשימת HCL (רשימת תאימות חומרה)

סיכום שיעור

שיעור זה סוקר כמה מהתקלות האופייניות העלולות להיווצר במהלך התקנת Windows 2000 Server. תקלות התקנה עלולות להיווצר ממדיה פגומה או חומרה לא תואמת. בנוסף, ייתכן שאין די מקום בשום מחיצה להתקנת Windows 2000 Server, כיון שלא השלמת את מטלות הקדם-התקנה. בעיות אחרות העלולות להתעורר הן חוסר יכולת להתחבר ל-Domain Controller או שלא ניתן להתקין או להתחיל את Windows 2000 Server.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות לשאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואח״כ בעברית.

The following questions are intended to reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A.

1. If you are installing Microsoft Windows NT, in a dual- boot configuration on the same computer, which file system should you choose? Why?

2. Which licensing mode should you select if users in your organization require frequent access to multiple servers? Why?

3. You are installing Windows 2000 Server on a computer that will be a member server in an existing Windows 2000 domain. You want to add the computer to the domain during installation. What information do you need, and what computers must be available on the network, before you run the Setup program?

4. You are using a CD- ROM to install Windows 2000 Server on a computer that was previously running another operating system. There is not enough space on the hard disk to run both operating systems, so you have decided to repartition the hard disk and install a clean copy of Windows 2000 Server. Name two methods for repartitioning the hard disk.

5. You are installing Windows 2000 over the network. Before you install to a client computer, what must you do?

6. A client is running Windows NT 3.5 Server and is interested in upgrading to Windows 2000. From the list of choices, choose all possible upgrade paths:

   Upgrade to Windows NT 3.51 Workstation and then to Windows 2000 Server.

   Upgrade to Windows NT 4.0 Server and then to Windows 2000 Server.

   Upgrade directly to Windows 2000 Server.

   Run Convert. exe to modify any NTFS partitions for file system compatibility with Windows 2000, and then upgrade to Windows 2000 Server.

   Upgrade to Windows NT 3.51 Server and then to Windows 2000 Server.

7. In your current network environment, user disk space utilization has been a major issue. Describe three services in Windows 2000 Server to help you manage this issue.

1. אם אתה מתקין Microsoft Windows NT בתצורת אתחול כפול על אותו מחשב, באיזה מערכת קבצים עליך לבחור? מדוע?

2. באיזה סוג סוג רישיון (Licensing Mode) עליך לבחור אם המשתמשים בארגון שלך צריכים גישה לעיתים קרובות למספר שרתים שונים? מדוע?

3. אתה מתקין Windows 2000 Server במחשב שיהיה שרת חבר בתחום Windows 2000 קיים. אתה רוצה להוסיף את המחשב לתחום בעת ההתקנה. איזה נתונים דרושים לך ואילו מחשבים צריכים להיות זמינים ברשת, לפני שתוכל להפעיל את תוכנית ההתקנה?

4. אתה משתמש בתקליטור להתקנת Windows 2000 Server על מחשב שהפעיל קודם מערכת הפעלה אחרת. אין די מקום על הדיסק הקשיח להפעיל את שתי מערכות ההפעלה, והחלטת לחצוץ את הדיסק מחדש ולהתקין העתק נקי של Windows 2000 Server. ציין שתי שיטות לחלוקה מחדש של דיסק למחיצות.

5. אתה מתקין Windows 2000 דרך הרשת. לפני שתתקין מחשב לקוח, מה עליך לעשות?

6. לקוח מפעיל Windows NT 3.5 Server ומעוניין לשדרג ל-Windows 2000. מרשימת האפשרויות בחר את כל אפשרויות השדרוג הנכונות:

   - שדרג לתחנת עבודה Windows NT 3.5 ואז ל-Windows 2000 Server.
   - שדרג ל-Windows NT 4.0 Server ואז ל-Windows 2000 Server.
   - שדרג ישירות ל-Windows 2000 Server.
   - הפעל Convert.exe לעדכון מחיצות NTFS לתאימות מערכת קבצים עם Windows 2000, ואז שדרג ל-Windows 2000 Server.
   - שדרג ל-Windows NT 3.51 Server ואז ל-Windows 2000 Server.

7. בסביבת הרשת הנוכחית שלך, נושא השימוש בשטח דיסק על ידי המשתמשים היה נושא מהותי. תאר שלושה שירותים במערכת Windows 2000 Server המסייעים לך לנהל נושא זה.

פרק 3

התקנות אוטומטיות של Windows 2000 Server

אודות פרק זה

לפישוט הליך התקנת Windows 2000 Server על מספר מחשבים, ניתן ליצור התקנה אוטומטית של מערכות הפעלה ויישומי שרת אחרים. לצורך כך, עליך ליצור ולהשתמש בקובץ תשובות, שהוא תוכנית ייעודית העונה על שאלות תוכנית ההתקנה באופן אוטומטי. לאחר יצירת קובץ זה, תוכל להפעיל את תוכנית ההתקנה משורת הפקודות, תוך שימוש באפשרויות המתאימות להתקנה אוטומטית. כך תוכל להתקין לא רק את מערכת ההפעלה Windows 2000 Server אלא גם יישומי שרת.

לפני שתתחיל

לביצוע השיעורים בפרק זה נדרש הציוד הבא:

- מערכת Windows 2000 Server מותקנת ופועלת על שרת Server01 כמתואר בפרק 2, תרגיל 1.
- מחשב שני מחובר ברשת למחשב Server01, ומפעיל גרסת 32 סיביות של מערכות הפעלה Windows 9x או Windows NT 3.51/4.0.
- בדוק היטב שהמחשב השני אכן מתאים לדרישות הסף של החומרה כמפורט בהקדמה.
- תקליטור ההתקנה של Windows 2000 Server.

שיעור 1:
הכנות להתקנה אוטומטית של Windows 2000 Server

בעת ביצוע התקנה אוטומטית של Windows 2000 Server, אתה יוצר קובץ תשובות המספק נתונים לשגרת ההתקנה. בנוסף, אם בכוונתך להתקין את Windows 2000 Server על מספר מחשבים דרך הרשת, עליך ליצור לפחות ערכה אחת של תיקיות הפצה. שיעור זה מפרט את הליך יצירת קובץ התשובות והגדרת תיקיות ההפצה הנדרשים להתקנה דרך הרשת.

לאחר שיעור זה, תוכל

- ליצור קובץ תשובות ייעודי להתקנה אוטומטית.
- להגדיר את ספריית ההפצה שלך להתקנת Windows 2000 Server דרך הרשת.

זמן לימוד משוער: 45 דקות

יצירת קובץ תשובות

קובץ התשובות הוא Script (תסריט) ייעודי (הנשמר לרוב כקובץ txt.) המאפשר הפעלת התקנה אוטומטית של Windows 2000 Server. הקובץ, הידוע לפעמים בשם Unattend File או Unattend Script File, עונה על השאלות של מנחה תוכנית ההתקנה בעת ההתקנה. הספריה i386\ בתקליטור ההתקנה של Windows 2000 Server מכילה דוגמה של קובץ תשובות, Unattend.txt, שתוכל לערוך ולהשתמש בהתקנה האוטומטית שלך. ניתן להשאיר את שם קובץ התשובות כפי שהוא, או לשנותו בהתאם לצרכי הארגון שלך. לדוגמה, השמות Comp1.txt, Install.txt ו-Setip.txt הם כולם שמות תקפים לקובץ תשובות כל עוד שמות אלה מוגדרים נכון בפקודת ההתקנה. היכולת להענקת שמות שונים מאפשרת בנייה ושימוש במספר קבצים כדי לתחזק מספר התקנות שונות באותו ארגון.

שים לב שתוכניות אחרות, כגון Sysprep.exe, העוזרות ליצירת דמות דיסק של התקנת Windows 2000 Server שלך, גם משתמשות בקובץ תשובות. (הנושא Sysprep נידון בפירוט בשיעור 2).

הטבלה הבאה מתארת מתן שם ושימוש בקובץ תשובות.

שם קובץ	מתי להשתמש בקובץ
<filename>.txt	בעת ביצוע התקנה אוטומטית. תוכל להשתמש בשם כלשהו עבור קובץ txt. Unattend.txt הוא שם קובץ הדוגמה הכלול במערכת Windows 2000 Server.
Winnt.sif	בעת התקנת Windows 2000 Server מתקליטור אתחול.
Sysprep.inf	בעת שימוש בכלי Sysprep ליצירת (Image) דמות דיסק עבור ההתקנה שלך של Windows 2000 Server.

פורמט זהה ל-Unattend.txt משמש עבור הקבצים שבטבלה מעלה. קובץ התשובות כולל קטעים אופציונליים רבים שניתן לשנות לאספקת נתונים עבור דרישות ההתקנה שלך. הקובץ מספק לתוכנית ההתקנה תשובות לכל השאלות הנשאלות בעת התקנה ידנית של Windows 2000 Server. בנוסף, קובץ התשובות מורה לתוכנית ההתקנה כיצד לנהוג בתיקיות וקבצי ההפצה שיצרת. לדוגמה, בקטע [Unattend] של קובץ התשובות, מופיעה שורה השואלת על התקנת ציוד של יצרן ציוד מקורי (OEM - **O**riginal **E**quipment **M**anufacture) ובה תסריט Preinstall המורה לתוכנית ההתקנה אם להעתיק את תת-התיקיות OEM מתיקיות ההפצה למחשב היעד.

פורמט קובץ התשובות

מבנה קובץ התשובות מכיל כותרות קטעים, מפתחות, וערכים לכל מפתח. רוב כותרות הקטעים מוגדרות מראש, אך חלקן ניתנות להגדרה על ידי המשתמש. המידע הבא כלול בקובץ Unattend.txt. ניתן להעתיק קובץ זה מהתקליטור למדיה אחרת שניתן לכתוב עליה, כגון דיסק קשיח, ואז לערוך את הקובץ כנדרש כדי שיתאים להתקנה האוטומטית שלך. תוכל גם לשנות את שם הקובץ.

Microsoft Windows 2000 Professional, Server, Advanced Server
and Datacenter
(c) 1994 - 1999 Microsoft Corporation. All rights reserved.
Sample Unattended Setup Answer File

This file contains information about how to automate the
installation or upgrade of Windows 2000 Professional and
Windows 2000 Server so the Setup program runs without
requiring user input.

```
[Unattended]
Unattendmode = FullUnattended
OemPreinstall = NO
TargetPath = WINNT
Filesystem = LeaveAlone
[UserData]
FullName = "Your User Name"
OrgName = "Your Organization Name"
ComputerName = "COMPUTER_NAME"

[GuiUnattended]
Sets the Timezone to the Pacific Northwest
Sets the Admin Password to NULL
Turn AutoLogon ON and login once
TimeZone = "004"
AdminPassword = *
AutoLogon = Yes
AutoLogonCount = 1
For Server installs

[LicenseFilePrintData]
AutoMode = "PerServer"
AutoUsers = "5"

[GuiRunOnce]
List the programs that you want to launch when the machine
is logged on to for the first time

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 70

[Networking]
When set to YES, setup will install default networking
components. The components to be set are
TCP/IP, File and Print Sharing, and the Client for Microsoft
Networks.
InstallDefaultComponents = YES

[Identification]
JoinWorkgroup = Workgroup
```

אם ההתקנה אינה דורשת את זה, אין צורך להגדיר את כל המפתחות האפשריים בקובץ תשובות. ערכי מפתחות לא נכונים עלולים ליצור שגיאות או התנהגות לא תקינה לאחר ההתקנה.

קובץ התשובות מחולק לקטעים. שם קטע מוכנס בסוגריים כמו בדוגמה הבאה:

[Userdata]

קטעים כוללים מפתחות וערכים תואמים למפתחות אלה. כל מפתח וערך מופרדים על ידי רווח, סימן שוויון, ורווח:

BitsPerPel = 8

ערכים הכוללים רווח בתוכם דורשים מרכאות כפולות:

OrgName = "Microsoft Corporation"

לקטעים אחדים אין מפתחות אלא רק רשימת ערכים:

[OEMBootFiles]
Txtsetup.oem

לשורות הערה יש נקודה ופסיק:

;Setup program runs without requiring user input.

מפתחות וערכים בקובץ תשובות

לכל מפתח בקובץ התשובות חייב להיות ערך משויך; אולם, חלק מהמפתחות אופציונליים, ולמפתחות אחרים יש ערך ברירת מחדל המשמש אם המפתח מושמט. ערכי מפתחות הם מחרוזות טקסט, אלא אם הם מוגדרים כערכים מספריים. אם הם הוגדרו כערכים מספריים, ערכם יהיה עשרוני אלא אם נאמר אחרת.

הערה המפתחות אינם רגישים לאות גדולה או קטנה **ויכולים להיכתב בשתיהן.**

קובץ Unattend.doc כולל מידע מפורט אודות מפתחות קובץ התשובות על תקליטור ההתקנה של Windows 2000 Server, תחת התיקיה \Support\Tools. להוצאה או צפייה בתוכן הקובץ Deploy.cab, השתמש בסייר Windows. לפרטים נוספים על פתיחת קובץ Unattend.doc, ראה קובץ Sreadme.doc שבתקליטור ההתקנה של Windows 2000 Server.

חשוב הפעלת Setup.exe **או** 2000rkst.msi מה**תיקיה** \Support\Tools **תתקין** את **כלי** התמיכה של Windows 2000 **בקובץ** Support.cab, **אך אינה פורסת את קובץ** Uattend.doc **או** כל קובץ **דחוס** אחר הנמצא ב-Deploy.cab.

שיטות ליצירת קובץ תשובות

תוכל ליצור קובץ תשובות באמצעות Setup Manager או על ידי יצירת הקובץ באופן ידני.

יצירת קובץ תשובות באמצעות Setup Manager

ליצירת ושינוי קובץ התשובות, השתמש ביישום Setup Manager שבתקליטור ההתקנה של Windows 2000 Server בתיקיה \Support\Tools\Deploy.cab. תוכל להשתמש ב- Setup Manager לביצוע המטלות הבאות:

- ❖ להגדיר את הפלטפורמה עבור קובץ התשובות (Windows 2000 Professional, Windows 2000 Server, Remote Operating System Installation או Sysprep).
- ❖ להגדרה של רמת האוטומציה של ההתקנה האוטומטית (Provide Defaults, Fully Automated, Hide Pages, Read Only ו- GUI mode attended Setup).
- ❖ להגדיר שם ברירת מחדל של משתמש ונתוני הארגון.
- ❖ להגדיר שם מחשב אחד או שמות מחשבים רבים לתמיכה בהתקנה אוטומטית על מחשבים רבים.
- ❖ להגדיר עד 99 התחברויות Administrators אוטומטיות להשלמת הליך ההתקנה.
- ❖ להגדיר הגדרות תצוגה.
- ❖ להגדיר הגדרות רשת.
- ❖ להגדיר התחברות לקבוצת עבודה או תחום ולהוסיף חשבון מחשב לתחום באופן אוטומטי.
- ❖ ליצור תיקיות הפצה.
- ❖ להוסיף פקודות לקטע [GuiRunOnce] של קובץ התשובות.
- ❖ ליצור קבצי טקסט Cmdlines.txt.
- ❖ להגדיר דפי קוד ועוד הגדרות ייחודיות-שפה.
- ❖ להגדיר הגדרות אזוריות.
- ❖ להגדיר אזור זמן.
- ❖ לציין נתונים של **T**elephony **A**pplication **P**rogramming **I**nterface (TAPI, ממשק יישום תכנות טלפוניה).
- ❖ להתאים אישית הגדרות דפדפן ו-Shell (מעטפת).

- להגדיר את שם תיקיית ההתקנה. מחיצת האתחול (המחיצה המכילה את קבצי מערכת ההפעלה) מוגדרת באמצעות מתג :t/ או \tempdrive:.
- להוסיף מדפסות.
- להוסיף מנהלי התקנים עבור התקני אגירה בנפחים גדולים, ולהוסיף HAL (**H**ardware **A**bstraction **L**ayer, שכבת הפשטת חומרה) אישית לשימוש בהתקנה אוטומטית.
- ליצור תיקיית הפצה ושיתוף עבור ההפצה או להגדיר שההתקנה האוטומטית תפעל מתקליטור ההתקנה של Windows 2000 Server.

בעזרת Setup Manager, תוכל להוסיף עקביות לתהליך יצירה או עדכון קובץ התשובות. אולם, לא תוכל להשתמש ב-Setup Manager לציון כל ההגדרות של קובץ התשובות, רכיבים אופציונליים, יצירת קבצי Txtsetup.oem, או יצירת תת-תיקיות בתיקיית ההפצה.

לאחר שהשתמשת ב- Setup Manager ליצירת קובץ תשובות, הוסף הגדרות נוספות באמצעות עורך כלשהו. עיין בקבצים Unattend.doc ו-Readme.txt שבקובץ Deploy.cab לרשימה מלאה של ההגדרות הזמינות.

הטבלה להלן מתארת את מפרטי Setup Manager הנפוצים ביותר.

פרמטר	מטרה
אפשרויות שדרוג	קובע אם להתקין את Windows 2000 Professional או Windows 2000 Server.
שם מחשב יעד	מציין את שם המשתמש, שם הארגון, ושמות המחשבים שיש להחיל על מחשבי היעד.
זיהוי מוצר (ID)	מציין את מספר רישוי המוצר הנלקח מתיעוד המוצר.
קבוצת עבודה או תחום	מציין את שם קבוצת העבודה או התחום אליה יש להוסיף את המחשב.
אזור זמן	מציין את אזור הזמן עבור המחשב.
נתוני תצורת הרשת	מציין את סוג מתאם הרשת ונתוני התצורה, כולל הפרוטוקולים של הרשת.

יצירת קובץ התשובות באופן ידני

ליצירה ידנית של קובץ התשובות, ניתן להשתמש בעורך כגון Notepad. באופן כללי, קובץ תשובות מורכב מכותרות קטעים, פרמטרים, וערכים עבור פרמטרים אלה. אף שרוב כותרות הקטעים מוגדרות מראש, ניתן גם להגדיר כותרות קטעים נוספות. שים לב שאין צורך לציין את כל הפרמטרים האפשריים בקובץ התשובות אם ההתקנה אינה דורשת אותם.

נספח B כולל קבצי תשובות לדוגמה המתאימים לתצורות התקנה מקובלות. ניתן לשנות ולהתאים את קובץ תשובות ברירת המחדל (Unattend.txt) המצורף ל-Windows 2000, או לכתוב קובץ חדש המבוסס על הדוגמאות בנספח זה.

יצירת תיקיות הפצה

להתקנת Windows 2000 Server על מספר מחשבים דרך הרשת, עליך ליצור לפחות ערכה אחת של תיקיות הפצה. בדרך כלל, תיקיות ההפצה שוכנות על שרת שאליו יכולים להתחבר מחשבי היעד. דבר זה מאפשר למשתמשים להתקין את Windows 2000 Server על ידי הפעלת Winnt.exe או Winnt32.exe על מחשבים אלה. ניתן להשתמש בערכת תיקיות הפצה אחת ומספר קבצי תשובות עבור יישומי מערכת שונים. גם אם אתה מתכוון להשתמש בהדמיית דיסק כשיטת ההתקנה שלך, התחלה עם תיקיות הפצה תעזור באספקת יישום אחיד עבור סוגי מערכות הפעלה שונים. בנוסף, תיקיות הפצה מאפשרות עדכון הדמיות עתידיות על ידי עריכת הקבצים בתיקיות ההפצה ליצירת הדמיות מעודכנות בלי צורך בהתחלה מחדש.

לסייע באיזון עומסים על פני השרתים ולהאיץ את שלב העתקת הקבצים של תוכנית ההתקנה של Windows 2000, תוכל ליצור תיקיות הפצה על מספר שרתים. תיקיות ההפצה יתמכו בהליך ההתקנה על מחשבים המפעילים מערכות הפעלה Windows 95, Windows 98, Windows NT, או Windows 2000. ניתן להפעיל את Winnt32.exe עם עד שמונה ערכות של תיקיות הפצה. כל ערכה של תיקיות הפצה כוללת את קבצי ההתקנה של Windows 2000 Server, בנוסף למנהלי התקנים כלשהם וקבצים אחרים הנדרשים להתקנה.

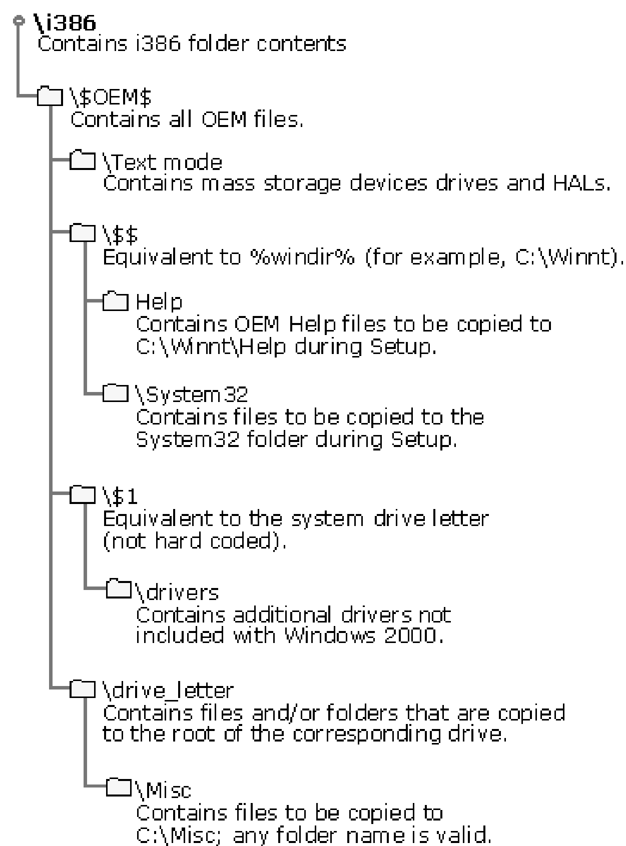
ליצירת תיקיית הפצה באופן ידני, חבר את שרת הרשת עליו ברצונך ליצור את תיקיית ההפצה, וצור תיקיה \W2kdist על שיתוף הרשת. לסייע באבחנה בין שיתוף מספר הפצות עבור המהדורות השונות של Windows 2000 (Windows 2000 Professional, Windows 2000 Server, Windows 2000 Advanced Server), בחר שמות שונים לכל תיקיה. אם נדרשות גרסאות בשפה מקומית של Windows 2000 עקב דרישות שלוחות בינלאומיות של הארגון שלך, תוכל להפריד שיתופי הפצה עבור כל גירסה מקומית. עבור כל מהדורה של Windows 2000, העתק את תוכן תיקיה \i386 לשיתוף ההפצה שנקבע עבורה. לדוגמה, אם אתה יוצר הפצה עבור Windows 2000 Server, צור ושתף תיקיה בשם \W2kdist והעתק את ספריית \i386 שבתקליטור ההתקנה של Windows 2000 Server.

הערה שיתוף ההפצה לתמיכה בהתקנת ברירת המחדל של Windows 2000 Server דורשת כ- 313MB חופשיים על הדיסק

ניתן גם להשתמש ב-Setup Manager ליצור ולשתף תיקיית הפצה באופן אוטומטי.

הגדרת מבנה תיקיית ההפצה

סעיף זה מספק מידע מפורט אודות התיקיות ותת-התיקיות המרכיבות את ערכת תיקיות ההפצה. תרשים 3.1 מתאר כיצד יש לבנות תיקיות אלה.



תרשים 3.1 דוגמה של מבנה תיקיות הפצה.

\i386 (תיקיה הנמצאת בתקליטור ההתקנה של Windows 2000, מועתקת לשיתוף ההפצה)

זו תיקיית ההפצה (Distribution Folder) העיקרית. היא מכילה את כל הקבצים הנדרשים להתקנת Windows 2000 Server. העתק את תכולת תיקיה זו מתקליטור ההתקנה של Windows 2000 Server לשורש של שיתוף ההפצה.

\OEM (תיקיה הנמצאת בשיתוף ההפצה, מועתקת ל-WIN_NT.~LS)

תת התיקיה \$OEM$ נמצאת ישירות מתחת לתיקיית ההפצה הראשית. בעת הפעלת תוכנית ההתקנה, ניתן להעתיק ספריות, קבצי Microsoft 8.3 (שם קובץ 8 תווים, סיומת 3 תווים) סטנדרטיים, וכל כלי אחר הדרוש להליך ההתקנה האוטומטי שלך, באופן אוטומטי ל-\$OEM$. שים לב שאם תשתמש במפתח OEMFILESPATH בקובץ התשובות, תוכל ליצור את תת התיקיה \$OEM$ מחוץ לתיקיית ההפצה.

\OEM מספקת את מבנה התיקיות הדרוש להעתקת קבצים נספחים למחשב היעד בעת ההתקנה. קבצים אלה כוללים מנהלי התקנים, תוכניות שירות, יישומים, וכל קובץ אחר הנדרש להפצת Windows 2000 Server בארגון.

\OEM עשויה להכיל את הקובץ האופציונלי Cmdlines.txt, הכולל רשימת פקודות להפעלה בשלב GUI Mode של ההתקנה. פקודות אלה יכולות לשמש להתקנת רכיבים אופציונליים, כגון כלים ותוכניות שירות. פקודות הכלולות ב-Cmdlines.txt מופעלות לפני שהמחשב מתחבר לרשת.

כל עוד תוכנית ההתקנה מאתרת את \$OEM$ בשורש נקודת ההפצה, היא תעתיק את כל הקבצים בספריה זו לספריה זמנית WIN_NT.~LS שנוצרה בשלב Text Mode של ההתקנה. בעת ההתקנה, תת תיקיות של \$OEM$ מועתקות למקום המתאים במחשב היעד. עם סיום ההתקנה, \$OEM$ וכל תת התיקיות נמחקות יחד עם WIN_NT.~LS.

הערה כל התיקיות המתוארות להלן ממוקמות על שיתף ההפצה תחת תיקיה \OEM, ומועתקות לאתרים שונים במחשב המפעיל את תוכנת ההעתקה.

\OEM\textmode (תיקיה המועתקת ל-WIN_NT~BT)

התיקיה \OEM\textmode מכילה קבצים חדשים או מעודכנים להתקנת Mass Storage Device Drivers (מנהלי התקנים להתקני אחסון גדולים מאוד) ו-HAL (שכבת הפשטת חומרה). קבצים אלה עשויים לכלול HAL של OEM (שכבת הפשטת חומרה של יצרן ציוד מקורי), מנהלי התקנים עבור התקני SCSI, וקובץ Txtsetup.oem, המבקר את הטעינה וההתקנה של רכיבים אלה.

כל הקבצים המונחים בתת התיקיה \OEM\textmode (מנהלי התקנים ו-HAL) צריכים להיות רשומים בקטע [OEMBootFiles] של קובץ התשובות.

\$oem$\$$ (תיקיה המועתקת ל- %windir% ולתת תיקיות של %windir%)

תת התיקיה \$OEM$\$$ תואמת לתכולת משתנה סביבתי %windir%. תת התיקיה כוללת את קבצי מערכת ההפעלה (קבצים חדשים או תחליפים לקבצי Retail) המועתקים לתת התיקיות השונות בעת התקנת Windows 2000. מבנה תיקיה זו חייב להתאים למבנה התקנת Windows 2000 סטנדרטית, בה \$OEM$\$$ תואמת את %windir%, \$OEM$\$$\System32 תואם את %windir%\System32 וכו'. כל תת תיקיה צריכה להכיל את הקבצים שיועתקו לתיקיה המתאימה של מערכת ההפעלה במחשב היעד.

הערה במערכת Windows 2000, %systemroot% **שווה ערך ל-** %windir%.

\$OEM$\$1\(תיקיה זו מועתקת ל- $Systemdrive$)

תת תיקיה \$OEM$\$1, החדשה עבור Windows 2000, מצביעה על הכונן בו מותקנת Windows 2000. $1 שווה ערך למשתנה הסביבתי %systemdrive%. לדוגמה, אם אתה מתקין את Windows 2000 על כונן :D, אז \$OEM$\$1 תצביע לעבר כונן :D. דבר זה מאפשר התקנת Windows 2000 בכוננים אחרים פרט ל- :C.

\$OEM$\$1\Drivers (תת תיקיה המועתקת ל-$systemdrive$\Drivers ולתת התיקיות של $systemdrive$\Drivers)

תת תיקיה \$OEM$\$1\Drivers, החדשה עבור Windows 2000, מאפשרת הכנסת מנהלי התקנים Plug and Play וקבצי התמיכה שלהם (קבצי קטלוג וקבצי התקנה INF.) בתת התיקיה Drivers ומתחתיה. תיקיות אלה על תוכנן, מועתקות לתיקיה %systemdrive%\Drivers במחשב היעד. הוספת הפרמטר OemPnPDriversPath לקובץ התשובות שלך, ינחה את Windows 2000 היכן לאתר את מנהלי התקנים Plug and Play החדשים או המעודכנים. בעת חיפוש מנהלי התקנים Plug and Play מתאימים להתקנה (בעת הפעלת תוכנית ההתקנה או מאוחר יותר), Windows 2000 מסתכלת בקבצים שבתיקיות שיצרת בנוסף לאלה שכלולים במערכת מההתחלה. שים לב שתוכל להחליף את השם בשם רצוי לך אחר, התואם את צורת מתן שמות MS-DOS 8.3 המקובלת.

הערה תת התיקיה \$OEM$\$1\Drivers מחליפה את תת התיקיות \Display **ו-** \Net המשמשות להתקנת Windows NT.

‎\$OEM$\$1\Sysprep (תת תיקיה המועתקת ל- %systemdrive%\Sysprep)

תת התיקיה \$OEM$\$1\Sysprep כוללת את הקבצים הנדרשים להפעלת תוכנית השירות Sysprep. Sysprep.exe ו-Sysprepcl.exe חייבים להיות בתיקיה %systemdrive%\Sysprep כדי ש- Sysprep יעבוד כנדרש.

טיפ הוסף את Sysprep.inf (הנוצר על ידי מנהל תוכנית ההתקנה או באופן ידני), לספריה \$OEM$\$1\Sysprep בשיתוף ההפצה. אחרת, נדרש דיסקט ובו קובץ Sysprep.inf להשלמה תקינה של ההתקנה באמצעות Sysprep.

התיקיה \OEM*drive_letter*

במצב טקסט (Text Mode), המבנה של כל תיקיית \$OEM$*drive_letter* מועתק בהתאמה לשורש של הכונן במחשב היעד. לדוגמה, קבצים שתניח בתת התיקיה \$OEM$\D מועתקים לשורש של כונן :D. תוכל גם ליצור תת תיקיות בתוך תיקיות אלו. לדוגמה, \$OEM$\E\misc גורמת לתוכנית ההתקנה ליצור תת תיקיה \Misc בכונן :E.

יש להכין רשימה של קבצים שנדרש לשנות את שמותיהם בקובץ $$Rename.txt. שים לב שלקבצים בתיקיית ההפצה צריכים להיות שמות קצרים (פורמט 8.3).

תרגיל 1: הכנת התקנה אוטומטית והפעלתה

בתרגיל זה, תיצור ותפעיל התקנה אוטומטית של Windows 2000 Server במחשב 2. להכנת ההתקנה האוטומטית, השתמש במנהל ההתקנה של Windows 2000 Server ליצירת קובץ תשובות ושיתוף הפצה על Server01.

אזהרה אין לשנות את שולחן העבודה או יישום כלשהו של Windows 2000 שעל Server01. אם תשנה, שלבים בתרגיל זה עלולים לא לפעול. לדוגמה, תרגיל זה תוכנן לפעול באמצעות לחיצה כפולה שהיא ההגדרה של ברירת המחדל של שולחן העבודה.

הליך 1: הפעלת Setup Manager (מנהל ההתקנה)

בצע הליך זה על Server01 כאשר תקליטור ההתקנה של Windows 2000 Server בכונן.

1. צור תיקיה בשם Deploy תחת C:\Program Files.
2. השתמש בסייר Windows, אתר את התיקיה \Support\Tools בתקליטור ההתקנה של Windows 2000 Server.

3. בחר בתיקיה TOOLS בחלונית התיקיות ולחץ לחיצה כפולה על סמל הקובץ Deploy בחלונית הימנית. כעת מופיעה תכולת קובץ הארכיון DEPLOY.

4. מתפריט Edit, בחר Select All.

5. מתפריט File, בחר Extract. יופיע חלון Browse For Folder (עיין למציאת תיקיה).

6. לחץ על סימן + משמאל ל-(Local Disk (C להרחבת כונן :C.

7. לחץ על סימן + משמאל ל- Program Files להרחבת התיקיה Program Files.

8. לחץ על התיקיה Deploy. התיקיה Deploy תיפתח.

9. לחץ OK. לרגע תופיע תיבת הודעות המודיעה על העתקה, בעוד קבצים מקובץ הארכיון DEPLOY נפרסים לתיקיה C:\Program Files\Deploy.

10. בתיקיה C:\Program Files\Deploy, לחץ לחיצה כפולה על setupmgr.

    Setup Manager יתחיל, ואשף Windows 2000 Setup Manager יופיע.

11. קרא את התיאור, ולחץ Next. יופיע מסך New Or Existing Answer File (קובץ תשובות חדש או קיים) ובו לחצן האפשרויות Create A New Answer File (צור קובץ תשובות חדש) נבחר.

12. לחץ Next. יופיע מסך Product To Install (מוצר להתקנה), ונבחר לחצן אפשרויות Windows 2000 Unattended Installation (התקנה אוטומטית של Windows 2000).

13. לחץ Next. יופיע מסך Platform ונבחר לחצן אפשרויות Windows 2000 Professional.

14. בחר לחצן אפשרויות Windows 2000 Server, ולחץ Next.

    יופיע מסך User Interaction Level, ונבחר לחצן אפשרויות Provide Defaults (ספק ברירות מחדל).

15. בחר את לחצן האפשרויות Fully Automated (אוטומטי לחלוטין), קרא את התיאור, ולחץ Next. יופיע מסך הסכם רשיון.

16. קרא את ההוראות על מסך זה. סמן את תיבת I Accept The Terms Of The License Agreement (אני מקבל את תנאי הרשיון), ולחץ Next.

    יופיע מסך Customize The Software (התאם את התוכנה באופן אישי).

17. בתיבת הטקסט Name, הקלד את שמך, והקש על מקש Tab.

18. בתיבת הטקסט Organization, הקלד את שם הארגון שלך או **MSPress Self-Study**, ולחץ Next. יופיע מסך הרשיון Licensing Mode וייבחר לחצן אפשרויות Per Server.

19. בחר את לחצן האפשרויות Per Seat (רשיון לפי מושב), ולחץ Next.

יופיע מסך Computer Names.

20. הכנס את התקליטור המצורף לספר ל-Server01, ולחץ Import (ייבוא). יופיע חלון Open.

21. ברשימה הנפתחת File Name, הקלד את הנתיב הבא (החלף את X באות המייצגת את כונן התקליטורים שלך):

X:\Books\59279\Chapt03\ex1\computer names.txt

ולחץ Open. יופיע מסך Computers Names ובו רשימת מחשבים שיש להתקין.

22. לחץ Next. יופיע מסך Administrator Password.

23. בתיבות הסיסמה, הקלד **password**, ובחר את תיבת הסימון When The Computer Starts, Automatically Log on As Administrator (כאשר המחשב מתחיל, התחבר אוטומטית כמנהל).

מספר הפעמים בהם ניתן להתחבר אוטומטית (Auto Logon) מוגדר 1.

24. לחץ Next. יופיע מסך Display Settings (הגדרות תצוגה).

25. השאר את כל תיבות הסימון במצב Use Windows Default (השתמש בהגדרות ברירת המחדל של Windows), ולחץ Next. יופיע מסך Network Settings. ולחצן אפשרויות Typical Settings יבחר.

26. לחץ Next. יופיע מסך Workgroup or Domain (קבוצת עבודה או תחום) ולחצן האפשרויות Workgroup נבחר.

עתה שרת Server01 מוגדר לתצורת חבר בקבוצת עבודה ששמה WORKGROUP. אי לכך, אין לשנות את הערכים המופיעים על מסך Workgroup or Domain. כאשר ההתקנה האוטומטית תופעל על המחשב השני, הוא ייהפך לחבר באותה קבוצת עבודה. בהמשך ההכשרה, Server01 ייהפך ל-DC (בקר תחום), והמחשב שעבורו אתה מכין קובץ תשובות, יצטרף ל-domain (תחום).

הערה **מאוחר יותר ניתן יהיה לשנות את קובץ התשובות שאתה מכין עכשיו, כך שיצטרף לתחום באופן אוטומטי וייצור חשבונות מחשבים בתחום. שינויים אלה מתבצעים באמצעות** Setup Manager **או עורך טקסטים.**

---

27. לחץ Next. יופיע מסך Time Zone (אזור זמן).

28. מהרשימה הנפתחת של אזורי זמן, בחר את אזור הזמן המתאים ולחץ Next.

יופיע מסך Additional Settings, ונבחר לחצן אפשרויות Yes, Edit The additional Settings (כן, ערוך את ההגדרות הנוספות).

29. לחץ Next. יופיע מסך Telephony.

30. ניתן להכניס את קידומות הארץ/אזור, עיר או כל קידומת נדרשת אחרת לחיוג חיצוני. אם למחשב השני אין גישה לחיוג חיצוני, התעלם ממסך זה והמשך.

31. לחץ Next. יופיע מסך Regional Settings, ובו מסומן לחצן האפשרויות Use The Default Regional Settings For The Windows Version You Are Installing (השתמש בהגדרות ברירת המחדל האזוריות לגרסת Windows שאתה מתקין).

32. לחץ Next. יופיע מסך Languages (שפות).

33. בחר בתמיכה בשפות נוספות שברצונך שיהיו זמינות עבור Windows 2000 Server, ולחץ Next. יופיע מסך Browser and Shell Settings, ובו נבחר לחצן אפשרויות Use Default Internet Explorer Settings (השתמש בהגדרות ברירת המחדל של Internet Explorer)

34. לחץ Next. יופיע מסך Installation Folder (תיקיית התקנה), ובו מסומן לחצן האפשרויות A Folder Named Winnt.

35. לחץ Next. יופיע מסך Install Printer (התקן מדפסת).

36. לחץ Next. יופיע מסך Run Once (הפעל פעם אחת).

37. בתיבת טקסט Command to Run, הקלד **Notepad.exe** ולחץ Add.

במצב רגיל, תיבת הטקסט Command To Run (פקודה שיש להפעיל) תכיל שורת קוד או תוכנה אחרת שתופעל להמשך ההגדרה של סביבת המשתמש. לצורך הכשרה, הפעלת Notepad ישמש את המטרה. שים לב, שאם הוספת מדפסת במסך הקודם, תופעל פקודת AddPrinter להוספת המדפסת לרשימת המדפסות המותקנות.

38. לחץ Next. יופיע מסך Distribution Folder.

39. בחר בלחצן אפשרויות Yes, Create Or Modify A Distribution Folder (כן, צור או שנה תיקיית הפצה), ולחץ Next.

יופיע מסך Distribution Folder Name, ובו נבחר לחצן האפשרויות Create A New Distribution Folder (צור תיקיית הפצה חדשה).

תוכן תיבת הטקסט Distribution Folder הוא C:\win2000dist, ותוכן תיבת הטקסט Share As Textbox הוא win2000dist.

40. לחץ Next. יופיע מסך Additional Mass Storage Drivers (התקני אחסון גדולים נוספים).

41. קרא את המסך ולחץ Next. יופיע מסך **H**ardware **A**bstraction **L**ayer (HAL, שכבת הפשטת החומרה)

42. קרא את המסך ולחץ Next. יופיע מסך Additional Commands (פקודות נוספות).

43. קרא את המסך ולחץ Next. פקודות המוקלדות כאן נכתבות בקובץ Cmdlines.txt. קובץ זה נוצר תחת תיקיית ההפצה בתת התיקיה OEM.

יופיע מסך OEM Branding.

44. לחץ Next. יופיע מסך Additional Files or Folders.

45. דפדף בתיקיות על ידי לחיצה עליהן וקריאת המידע המופיע תחת Description.

לחץ Next. יופיע מסך Answer File Name ובו שם הקובץ והנתיב שבתיבת הטקסט Location and File Name בתקליטור.

46. ודא ששם הקובץ והנתיב הם **C:\Win2000dist\Unattend.txt**, ולחץ Next.

יופיע מסך The Location Of Setup Files (מיקום קבצי ההתקנה), ונבחר לחצן אפשרויות Copy The Files From CD (העתק את הקבצים מתקליטור).

47. הוצא את התקליטור המצורף לספר זה, והכנס במקומו את תקליטור ההתקנה של Windows 2000 Server.

לאחר שתקליטור ההתקנה של Windows 2000 Server נקרא, יופיע מסך Microsoft Windows 2000 CD.

48. סגור את מסך Microsoft Windows 2000 CD.

49. לחץ על Next במסך Location of Setup Files.

יופיע מסך Copying Files בעוד קבצים מועתקים מספריית i386\ שבתקליטור ההתקנה ל- C:\Win2000Dist.

50. אפשר להעתקת הקבצים להסתיים, לפני שאתה עובר להליך הבא.

לאחר סיום מטלות Setup Manager, יופיע אשף Completing The Windows 2000 Setup Manager.

51. קרא את המסך ולחץ Finish.

הליך 2: בדיקה של תיקיית ההפצה שנוצרה על ידי מנהל ההתקנה

בהליך זה, תבדוק את מבנה התיקיות שנוצר על ידי Setup Manager, את קובץ התשובות (Unattend.txt), קובץ UDF (Unattend.udf), וקובץ אצווה (Unattend.bat).

1. לחץ על Start ואחר כך על Run. תופיע תיבת הדו-שיח של Run.
2. בתיבת טקסט Open, הקלד C:\Win2000dist ולחץ OK. יופיע חלון Win2000dist.
3. פתח חלון נוסף לספריה הבאה שבתקליטור ההתקנה של Windows 2000: <cd-rom drive:>\i386. יופיע חלון i386.
4. סדר את החלונות כך שתוכל לצפות בחלון Win2000dist ובחלון i386.
5. איזו תיקיה מופיעה ישירות מתחת לתיקיה Win2000dist שאינה מופיעה בתיקיה i386?
6. בדוק את מבנה הספריה שמתחת oem ועיין בתרשים 3.1 בטקסט. בשאלות הסיכום שבסוף פרק זה, תישאל שאלה בקשר למבנה זה.
7. חזור לתיקיה Win2000dist, ואתר את שלושת קבצי Unattend.

   שים לב ששניים מקבצי Unattend מופיעים ללא סיומת.
8. כדי לראות את הסיומות של כל הקבצים, גש ל-Tools ובחר Folder Options.

   תופיע תיבת הדו-שיח Folder Options.
9. לחץ על הכרטיסיה View.
10. מתיבה Advanced Settings, הסר סימון מתיבת סימון Hide File Extensions For Known File Type (הסתר סיומות קובץ עבור סוגי קבצים ידועים), ולחץ OK.
11. אתר את קבצי Unattend שנית. קבצי Unattend יופיעו כאשר הסיומות שלהם גלויים.

    בחר Unattend.txt, ומתפריט File , בחר Open. Unattend.txt יופיע ב-Notepad.
12. אתר את קטע [User Data] והוסף שורה בשם ProductID+<*your_product_key*>. עבור ערך ProductID, הקלד את קוד המוצר (Product Key) של המוצר המסופק עם העותק שלך של Windows 2000 Server.
13. שמור וסגור את Unattend.txt.
14. לקבלת הסברים על קטע כלשהו בקובץ זה, פנה ל- Unattend.doc הנמצא בתיקיה C:\Program Files\Deploy שיצרת בתחילת תרגיל זה. ניתן לפתוח את הקובץ Unattend.doc באמצעות Microsoft Wordpad, Microsoft Word, או כל מעבד תמלילים אחר המסוגל לקרוא קבצי Microsoft Word.

15. סגור את קובץ Unattend.doc.

16. בחר Unattend.udf מחלון Win2000dist; בחר Open With מתפריט File.

תיבת הדו-שיח Open With תופיע.

17. בחר Notepad מתיבת Choose The Program You Want To Use (בחר את התוכנה שתשמש אותך), ולחץ OK.

שים לב ש- 12 שמות המחשבים שיובאו בפעולת Setup Manager, מופיעים כאן.

18. מה היא מטרת קובץ UDF?

19. סגור את קובץ UDF.

20. מחלון Win2000dist, בחר Unattend.bat; מתפריט File, בחר Edit.

תכולתו של קובץ האצווה מופיעה ב- Notepad.

21. שים לב שקובץ האצווה מגדיר משתנים, ומשתנים אלה משמשים להפעלת Winnt32 עם מתגים. כמו כן, שים לב שעליך לציין את שם המחשב בעת קריאה לקובץ האצווה כיון שקובץ UDF משתתף בשגרת ההתקנה.

22. סגור את חלון Unattend.bat.

הערה כאשר משתמשים במתג UDF/ להגדרת ערכים ייחודיים, יש לציין את שם קובץ UDF. הסיומת של קובץ UDF השתנתה ממערכת Windows NT (במערכת NT יצרנו קובץ טקסט UDF_name.TXT) ובמערכת Windows 2000 מגדירים סיומת udf או udb.

כאשר משתמשים בתוכנת Setup Manager ליצירת קובץ UDF עבור הגדרת שמות מחשב שונים, יוצרת התוכנה קובץ Unattend.udf. אולם, במידה ולא ציינו את שם קובץ UDF לאחר מתג UDF/, תנחה אותנו מערכת ההתקנה להכניס דיסקט המכיל קובץ $unique$.udb. במקרה זה, הסיומת של הקובץ חייבת להיות udb.

הליך 3: הפעלת התקנה אוטומטית של Windows 2000 Server ממחשב 2.

על המחשב השני צריכה להיות מותקנת כבר מערכת הפעלה 32 סיביות, כגון Windows 95 או Windows NT. בנוסף, שרת Server01 חייב להיות מחובר לאותה רשת של המחשב השני. כל הדרישות עבור התרגיל מפורטות בהקדמה.

אזהרה אם המחשב השני מפעיל Windows NT, מחיצת האתחול שלו היא \:C, וספריית מערכת ההפעלה שלו היא Winnt, שנה את שם ספריית ההתקנה ב-Unattend.txt. שם הספריה הרשום ב- Unattend.txt נמצא בקטע Unattend, ושם הערך (Valuename) הוא TargetPath. לדוגמה, שנה את הערך ל- TargetPath=\WIN2000S.

---

1. מהמחשב השני, מפה אות כונן (:H ישמש במהלך תרגיל זה), ל-Server01\WIN2000dist\\. תוכל להתחבר לשרת Server01 על ידי שימוש בשם משתמש של ה-administrator וסיסמה password.

הערה אם אתה פועל תחת Windows 9x, ונתקל בקשיים בהתחברות לשרת Server01, ודא שהמחשב הוא חבר בקבוצת עבודה, והתחבר כ-administrator עם הסיסמה password.

---

2. פתח מנחה פקודה והקלד **:cdh**

אזהרה אם שדרגת מ-Windows 9x, ייתכן שתוכנית ההתקנה לא תוכל לאתר קובץ udf. אם כך קורה, פתח את Unattend.bat בשרת Server01 והגדר את הנתיב המלא של קובץ udf.

---

3. ממנחה הפקודה, הקלד H:\Unattend Server02.

4. יופיע מסך Copying Installation Files בעוד Windows 2000 Server מפעיל התקנה אוטומטית דרך הרשת.

   עם סיום שלב זה, יופיע מסך המתריע שהמחשב יאתחל מחדש.

הערה ניתן להשלים שלב לפני-טקסט זה של תוכנית ההתקנה באמצעות מתג syspart/ עם Winnt32.exe.

---

5. אפשר למחשב לאתחל מחדש.

בעת האתחול, יופיע תפריט אתחול Windows 2000, ותוכנית ההתקנה של Windows 2000 Server תמשיך ותעבור למצב טקסט.

המחשב מאתחל שנית, ותפריט האתחול מופיע ובו נראה Windows 2000 Server.

תוכנית ההתקנה של Windows 2000 תמשיך לחלק הגרפי של ההתקנה. מסכים Installing Devices (התקנת התקנים) ו-Installing Components (התקנת רכיבים), אורכים זמן עד לסיום. עתה יופיע מסך Performing Final Tasks (מבצע מטלות אחרונות), בו Windows 2000 Server משלימה את שגרת ההתקנה. עם סיום ההתקנה, מסך Windows 2000 Setup יודיע שהמחשב יאתחל מחדש.

6. לאחר שהמחשב חוזר ומתחיל, שים לב שהוא מתחבר אוטומטית כ-Administrator כפי שהוגדר ב-Setup Manager. בשלב זה המדפסת מותקנת וקובץ Notepad.exe פועל.

7. סגור את Noptepad. יופיע מסך Windows 2000 Configure Your Server (הגדר מסך של Windows 2000)

8. בחר בלחצן האפשרויות I Will Configure This Server Later (אגדיר שרת זה מאוחר יותר), ולחץ Next. יופיע מסך Configure Your Server.

9. הסר סימון מתיבת סימון Show This Screen At Startup (הראה מסך זה בהתחלה), וסגור את המסך.

אזהרה אם אתה משדרג מ-Windows 9x **ולא ביקשת הסבת מחיצת ההתקנה למערכת** קבצים NTFS בזמן ההתקנה, תצטרך להסב אותה ידנית על ידי הקלדת הפקודה Convert C:\Fs:Ntfs **בשורת הפקודה.**

סיכום שיעור

לפני שתוכל לבצע התקנה אוטומטית של Windows 2000 Server, עליך ליצור קובץ תשובות, שהוא קובץ פקודות ייעודי הכולל מספר קטעים אופציונליים, אותם אתה מעדכן כדי לספק מידע על דרישות ההתקנה שלך. הקובץ מספק תשובות לתוכנית ההתקנה לכל השאלות הנשאלות בעת התקנה ידנית של Windows 2000 Server. בנוסף, קובץ התשובות מורה לתוכנית ההתקנה איך לפעול מול קבצי ההפצה והקבצים שיצרת. עליך ליצור לפחות ערכת קבצי הפצה אחת להתקנת Windows 2000 Server דרך הרשת. שימוש ב-Setup Manager יכול ליצור תיקיית הפצה וקובץ תשובות באופן ידני או אוטומטי. כדי להמשיל ולהתאים את קובץ התשובות, עיין בקובץ Unattend.doc שבתקליטור ההתקנה של Windows 2000 Server.

שיעור 2:
יצירת מערך אוטומטי להתקנת Windows 2000 Server

התקנות אוטומטיות של Windows 2000 Server כרוכות בהפעלת תוכנית ההתקנה עם קובץ תשובות. תוכל לבצע התקנות אוטומטיות על מספר מחשבים, כך שתוכנית ההתקנה תוכל להתבצע בצורה אוטומטית. ניתן ליצור מערך התקנה אוטומטי עבור ההתקנות הבאות:

- ליבת מערכת ההפעלה של Windows 2000 Server.
- כל יישום שאינו פועל כ-שירות.
- תמיכה בשפות נוספות עבור Windows 2000 Server על ידי התקנת מיגוון ערכות שפה.
- חבילות שירות (Service Packs) עבור Windows 2000 Server.

שיעור זה מתמקד בהתקנה אוטומטית של מערכת ההפעלה של Windows 2000 Server. ללמוד על התקנות אוטומטיות של יישומים אחרים, ראה שיעור 3 "יצירת מערך אוטומטי להתקנת יישומי שרת".

לאחר שיעור זה, תוכל

- לבצע התקנה אוטומטית של מערכת ההפעלה Windows 2000 Server.

זמן לימוד משוער: 45 דקות

ביצוע התקנה אוטומטית

לביצוע התקנה אוטומטית של Windows 2000 Server, עליך להגדיר את קובץ התשובות לפני הפעלת תוכנית ההתקנה. ישנם שלושה סוגים בסיסיים של התקנות אוטומטיות להתקנת Windows 2000 Server: שיטת תקליטור האתחול, שיטת Winnt.exe, או שיטת Winnt32.exe.

תקליטור האתחול

כדי להתחיל התקנה אוטומטית של Windows 2000 Server מתקליטור, יש לוודא קיום התנאים הבאים:

- על המחשב לתמוך בתקליטור אתחול בפורמט El Torito (ללא מצב הדמיה) כדי לאתחל מכונן התקליטורים.
- קובץ התשובות חייב להיקרא Winnt.sif ולהיות מותקן על דיסקט שיש להכניסו לכונן הדיסקטים מייד עם אתחול המחשב מהתקליטור.
- על קובץ התשובות להכיל קטע [Data] ובו מוגדרים המפתחות הנדרשים.

Winnt.exe או Winnt32.exe

פקודת Winnt.exe הבאה מהווה דוגמה ליישום התקנה אוטומטית:

Winnt /S:Z:\i386 /u:Z:\unattend.txt /t:c

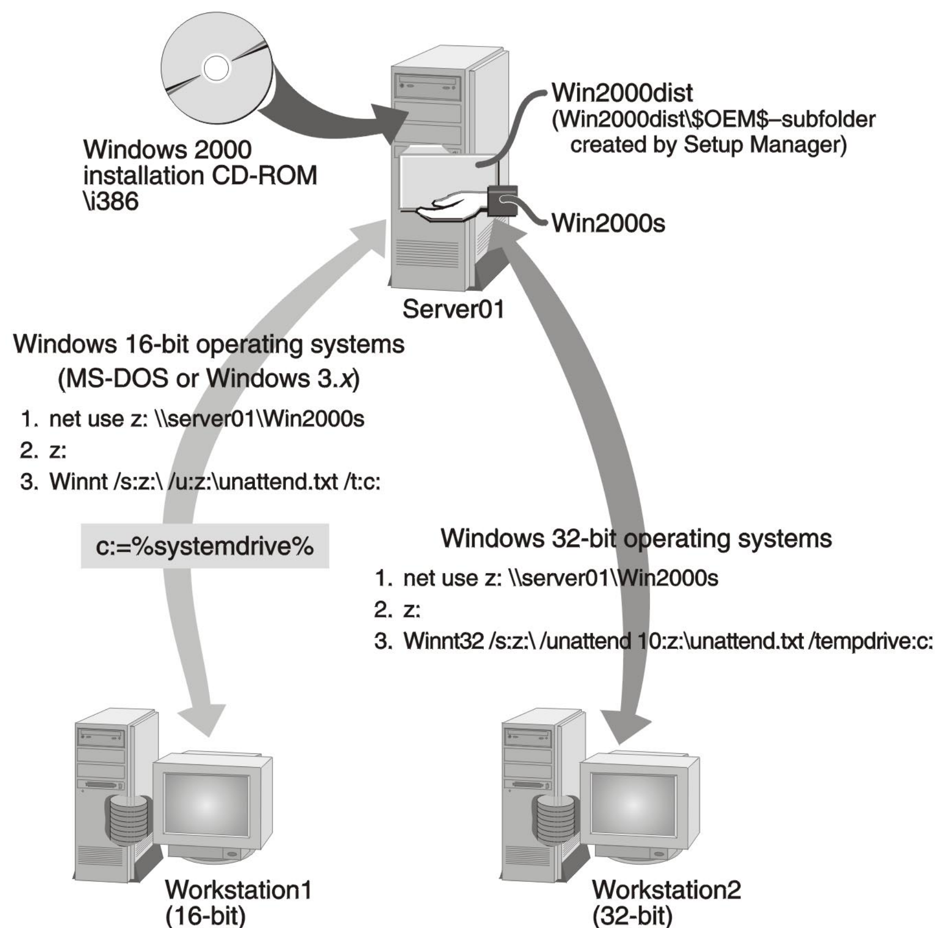
שים לב לשימוש במתג /u: בשורת הפקודה, המעיד על התקנה אוטומטית. מתג /t: מעיד לאיזה כונן תוכנית ההתקנה תעתיק את קבצי המקור להמשך ההתקנה. Z:\i386 הוא המיקום ברשת המכיל את קבצי המקור של התקנת Windows 2000. על המחשב המקומי למפות את כונן Z: לשיתוף הרשת שבו נמצאת תת התיקיה i386, לפני ששורת פקודה זו, המהווה דוגמה, תעבוד כיאות.

פקודת Winnt32.exe הבאה מהווה דוגמה דומה לפקודת Winnt הקודמת, לצורך יישום התקנה אוטומטית:

Winnt32 /S:Z: \i386 /unattend 10:Z: \unattend.txt /tempdrive:c

Winnt32.exe משתמש ב- /unattend: במקום /u: להפעלת ההתקנה האוטומטית. המספר שבא אחרי מתג /unattend: מודיע לשגרת ההתקנה כמה זמן עליה לחכות לאחר העתקת קבצים כדי לבצע אתחול חוזר של המחשב ולהמשיך בתוכנית ההתקנה. פקודת num פועלת על Windows NT או Windows 2000 אך מחשבים המפעילים מערכות הפעלה Windows 9x מתעלמים ממנה.

תרשים 3.2 מפרט את הצעדים הנדרשים להפעלת ההתקנה האוטומטית שבדוגמאות הקודמות.



תרשים 3.2 ייזום התקנה אוטומטית במחשבים בעלי מערכות הפעלה 16 סיביות ו- 32 סיביות.

יצירת מערך אוטומטי להתקנת Windows 2000 Server

ישנן מספר שיטות ליצירת מערך אוטומטי להתקנת Windows 2000 Server. השיטה בה תשתמש תלויה בתוצאה הנדרשת. במצבים מסוימים, ניתן לשלב בין כמה שיטות. לדוגמה, Syspart ו- Sysprep יכולים לשמש יחד בתסריטי התקנה מסוימים.

בנוסף לשיטות ההתקנה הבסיסיות המתוארות לעיל, תוכל להשתמש גם בשיטות הבאות לביצוע התקנה אוטומטית של Windows 2000 Server :

- תוכנית ההתקנה Winnt32.exe יחד עם פרמטר /syspart.
- כלי הכנת המערכת (System Preparation Tool, Sysprep).

❖ שרת ניהול המערכת (**S**ystem **M**anagement **S**erver - SMS).

❖ תקליטור אתחול.

❖ שירות התקנה מרחוק (**R**emote **I**nstallation **S**ervice - RIS).

שיטות אלו מבוססות על שיטות ההתקנה דרך הרשת שפורטו מעלה, או מחליפות אותן. הטבלה הבאה מפרטת מתי להשתמש בכל שיטת התקנה:

שיטת התקנה	**שימוש**	**שדרוג**	**התקנה חדשה**
Syspart	השתמש ב-Syspart להתקנות חדשות במחשבים בעלי חומרה שונה.	לא	כן
Sysprep	השתמש ב-Sysprep כאשר החומרה של המחשב הראשי ושל מחשב היעד זהות, כולל HAL והתקני האחסון הגדולים.	לא	כן
SMS	השתמש ב-SMS לשדרוג מבוקר של מספר מערכות Windows 2000 Server, במיוחד כאשר הן מרוחקות גיאוגרפית אחת מהשנייה.	כן	כן
תקליטור אתחול	השתמש בשיטת תקליטור אתחול עבור מחשב שה-BIOS שלו מאפשר אתחול מתקליטור.	לא	כן
שירות התקנה מרחוק (RIS)	השתמש ב-RIS במחשב התומך ב-PXE או דיסקט אתחול RIS. שתי השיטות מאפשרות למחשב להתחבר לשרת RIS מרושת בהליך האתחול הראשוני ולקבל התקנה של Windows 2000 Professional. Pre-Boot Execution Enviroment (PXE), סביבת הפעלה טרום-אתחול), מאפשרת למחשב שבו PXE ROM לאתחל לשרת הרשת. PXE ROM מקודד לתוך ה-BIOS או ממוקם על NIC כ-ROM אופציונלי.	לא	כן

הערה בעת כתיבת ספר זה, RIS מסוגל לבצע התקנה אוטומטית של Windows 2000 Professional בלבד. הוא אינו תומך בהתקנה אוטומטית של Windows 2000 Server. שיפורים עתידיים של RIS עשויים לאפשר התקנה אוטומטית של Windows 2000 Server ומערכות הפעלה אחרות.

הטבלה מפרטת גם איזו שיטת התקנה משמשת לשדרוג או התקנה חדשה. לפני שתיצור מערך אוטומטי להתקנת Windows 2000 Server, עליך להחליט אם ההתקנה היא שדרוג של Windows NT או התקנה חדשה.

אם תבצע התקנה חדשה, שים לב שכיון שהתקנה אוטומטית היא בלתי מאוישת, התקנה חדשה יכולה להחליף מחיצות קיימות או קבצים במחיצות קיימות. קבצי יישומים וקבצי נתונים יכולים להישאר על מחיצות, אף שיש להתקין יישומים מחדש כדי לרשום אותם במערכת ההפעלה החדשה.

שימוש ב-Syspart

Syspart מופעלת על ידי הכללתה כפרמטר בתוכנית ההתקנה Winnt32.exe. Winnt32 עם מתג Syspart מופעלת על Reference Computer (מחשב ייחוס) להשלמת השלב הראשון של ההתקנה. אם למחשב הייחוס ולמחשבים עליהם תתקין את Windows 2000 Server אין חומרה זהה, תוכל להשתמש בשיטת Syspart. שיטה זו מפחיתה את זמן ההפצה על ידי השלמת שלב העתקת הקבצים על מחשב הייחוס, ובכך מבטלת שלב זה במחשבים המיועדים להתקנה.

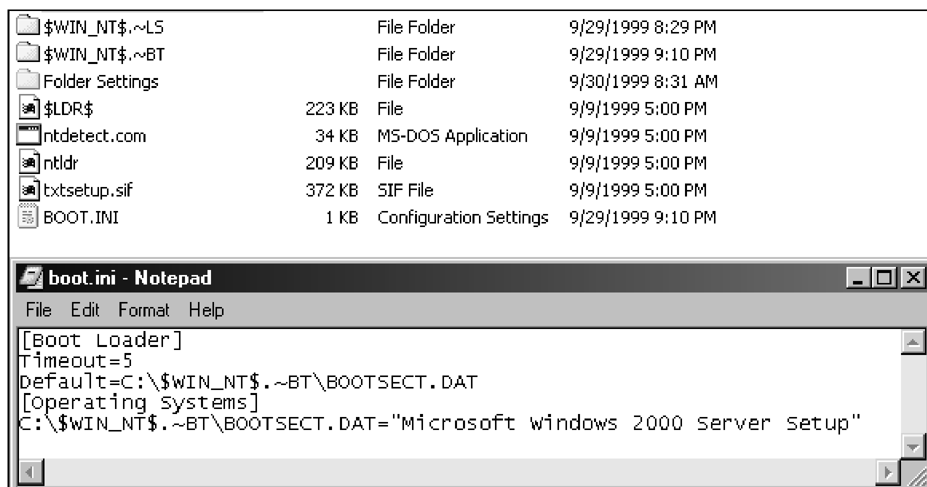
Syspart דורשת שתשתמש בשני דיסקים פיסיים, כאשר המחיצה הראשית היא על דיסק היעד. אולם, דיסק היעד אינו חייב להיות ממוקם במחשב הראשי. הוא יכול להיות על מחשב אחר ברשת, כל עוד הוא דיסק נקי שאין עליו מערכת הפעלה.

אם נדרשת התקנה דומה ומערכת הפעלה דומה על סוגי חומרה בהן HAL ובקרי האחסון הגדולים שונים, תוכל להשתמש ב-Syspart ליצירת ערכת קבצי הורה עם נתוני תצורה הנדרשים ותמיכה במנהלי התקנים. ערכת קבצי הורה זו יכולה לשמש על מערכות לא זהות כדי לאתר את החומרה כנדרש ולהגדיר את מערכת ההפעלה הבסיסית בצורה אחידה.

לאחר שמחשב הייחוס פועל, התחבר לתיקיית ההפצה והפעל את תוכנית ההתקנה על ידי הפעלת תוכנית Winnt32.exe משורת הפקודה:

```
winnet32 /unattend:unattend.txt /s:install_source /
syspart:install_target /tempdrive:install_target /noreboot
```

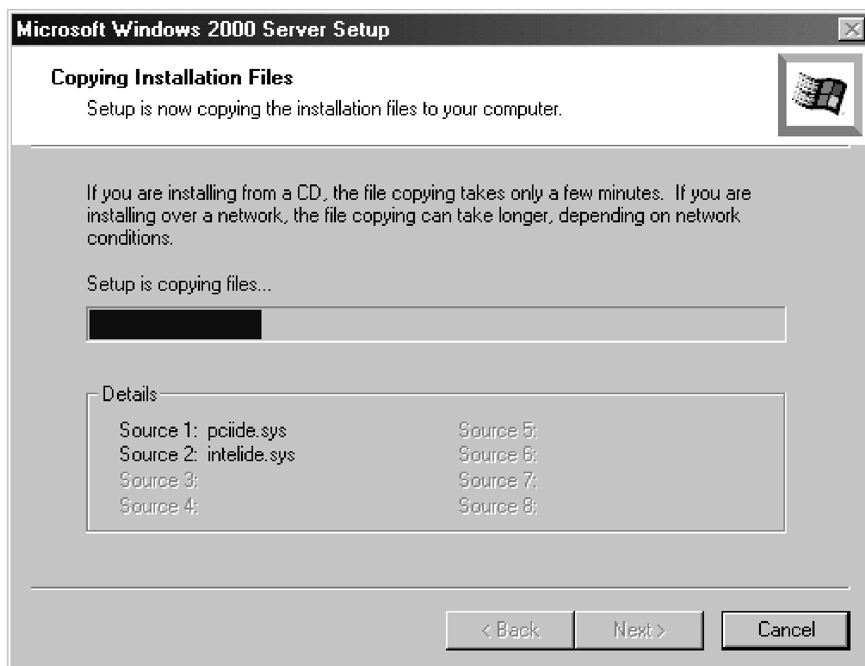
לאחר הפעלת הפקודה הקודמת בה install_target שווה D, המבנה שלהלן נוצר על כונן :D (תרשים 3.3).



תרשים 3.3 תכולת דיסק :D ו- Boot.ini של מחשב היעד, לאחר הפעלת Syspart.

להלן מידע נוסף על הפרמטרים והערכים המשמשים בעת הפעלת תוכנית ההתקנה Winnt32.exe :

- ❖ ערך Unattend.txt הוא קובץ התשובות המשמש להתקנה אוטומטית. הוא מספק תשובה לחלק או כל שאלות המנחים אליהם מגיב משתמש הקצה בעת ביצוע התקנה מאוישת. השימוש בקובץ תשובות הוא אופציונלי בעת יצירת ערכת קבצי אב.
- ❖ ערך **install_source** הוא המיקום של קבצי Windows 2000 Server. הגדר מתגי /s רבים בשורת הפקודה אם ברצונך להתקין ממספר מקורות בו זמנית. תרשים 3.4 מתאר העתקת קבצים הנערכת משני מקורות. המקור הראשון הוא כונן רשת, המקור השני הוא כונן תקליטור מקומי. כפי שמתואר בתרשים, ניתן להגדיר עד שמונה מקורות התקנה.



תרשים 3.4 מסך Copy Installation Files ובו שני מקורות להעתקת קבצים.

- פרמטרים /syspart ו- /tempdrive חייבים להצביע למחיצה זהה של דיסק קשיח משני. התקנת Windows 2000 Server חייבת להתבצע על מחיצה ראשית של דיסק קשיח משני זה. Syspart תגדיר את המחיצה כפעילה, כך שהיא תהיה בת-אתחול.
- חובה להשתמש בפרמטר /tempdrive כדי שהתקנה באמצעות Syspart תהיה מוצלחת. בעת שימוש במתג שורת הפקודה /tempdrive, ודא שיש די מקום פנוי על הדיסק במחיצה השניה להתקנת Windows 2000 Server וקובץ ההתקנה שהוא יוצר על WIN_NT.~LS.
- ערך **install_drive** הוא המחיצה המכילה את קדם-ההתקנה של Windows 2000 Server. הקבצים בכונן זה מפורטים בתרשים 3.3.

הערה Syspart יסמן את הכונן כפעיל אוטומטית כהכנה להעברתו למחשב היעד.

שימוש ב-Sysprep

Sysprep הוא כלי המסייע ביצירת דמות הדיסק (Disk Image) של התקנת Windows 2000 Server. שכפול דיסקים הוא בחירה טובה, אם נדרשות התקנות רבות בתצורה זהה. כדי להשתמש בכלי Sysprep, עליך להתקין את Windows 2000 Server על מחשב ייחוס. גם כל יישום אחר שיידרש על מחשב היעד, יש להתקין על מחשב הייחוס. עתה הפעל את Sysprep ואחר כך תוכנית שירות להדמיית דיסק (Imaging).

Sysprep תכין את הדיסק הקשיח על מחשב ההורה כך שתוכנית השירות להדמיית הדיסק תוכל להעביר את דמות הדיסק למחשבים אחרים. שיטה זו מפחיתה את זמן ההתקנה בצורה דרמטית בהשוואה לשיטות הסטנדרטיות או המקודדות.

טיפ צור תקליטור **ובו** דמות הדיסק או העבר את הדיסק לאתר מרושת כדי שניתן יהיה להשתמש בדמות להתקנה מהירה של מחשבים זהים או כמעט זהים.

כדי להשתמש ב-Sysprep למחשב ההורה ומחשבי היעד חייב להיות HAL, תמיכת **A**dvanced **C**onfiguration And **P**ower **I**nterface - ACPI, והתקני אחסון גדולים זהים. Windows 2000 מאתרת התקני הכנס-הפעל באופן אוטומטי, ו-Sysprep חוזרת מאתרת ומקדדת (Re-enumerate) את ההתקנים במערכת ההפעלה בעת הפעלת המחשב לאחר הפעלת Sysprep. מכאן נובע שהתקני הכנס-הפעל, כגון כרטיסי רשת, מודמים, מתאמי תצוגה וכרטיסי קול, לא חייבים להיות זהים על מחשב ההורה ומחשבי היעד. היתרון העיקרי בהתקנה באמצעות Sysprep הוא המהירות. ניתן לארוז ולדחוס את הדמות ורק הקבצים הנדרשים עבור ההתקנה הנתונה נוצרים כחלק מהדמות. התקני הכנס-הפעל הנדרשים במערכות אחרות נוצרים גם. ניתן להעתיק את הדמות לתקליטור ולהפיצה לאתרים רחוקים אליהם קיימת תקשורת איטית.

הערה כיון ש-HAL, תמיכת ACPI, והתקני האחסון הגדולים במחשב ההורה ומחשבי היעד חייבים להיות זהים, ייתכן שתצטרך לשמור מספר דמויות עבור סביבת העבודה השונות שלך.

Sysprep מאפשרת הגדרת דמות הורה ובה הרכיבים הנדרשים עבור שרת חבר ומאוחר יותר להגדיר את השרת, ואם נדרש, לקדמו לרמת DC. דבר זה ניתן לעשות באופן ידני או על ידי הפעלת הפקודות בקטע [GuiRunOnce] של קובץ Sysprep.inf. למידע נוסף אודות קובץ Sysprep.inf, ראה סעיף "קבצי Sysprep" בהמשך פרק זה.

אם סביבת העבודה שלך כוללת מספר סוגי מערכות תלויות-חומרה, תוכל להשתמש ב-Sysprep יחד עם Syspart ליצור הורה לכל סוג. לעשות כן, התקן Windows 2000 על מחשב אחד מכל סוג, ואז השתמש בתוכנית השירות Sysprep ליצירת הדמיות שישמשו להתקנה במחשבים הנותרים מכל סוג. למידע נוסף אודות Sysprep, עיין בסעיף "שימוש ב-Sysprep להרחבת מחיצות בדיסק", בהמשך שיעור זה.

לפני שתתחיל, בחר במחשב שישמש כמחשב ייחוס. מערכות Windows NT Server או Windows 2000 Server חייבות להיות מותקנות במחשב הייחוס.

הערה ניתן להשתמש ב-Sysprep גם ליצירת התקנות של Windows 2000 Professional.

הליך העבודה עם Sysprep

המידע להלן הוא סקירה על הליך בניית מחשב מקור שישמש לשכפול Sysprep.

- **התקנת Windows 2000** –יש להתקין את Windows 2000 Server על מחשב בעל חומרה דומה למחשבי היעד. אין לחבר את המחשב לתחום בעת הרכבתו. בנוסף, סיסמת ה-Administrator המקומי צריכה להישאר ריקה.
- **הגדרת המחשב** – עליך להיות מחובר כ-Administrator בעת התקנה והתאמת Windows 2000 Server ויישומים משויכים. עליך לכלול IIS, או להתקין ולהגדיר שירותים אחרים.
- **בדיקת הדמות** – עליך להפעיל ביקורת לקוח (Client Audit), המבוססת על הקריטריונים שלך, לוודא שתצורת הדמות נכונה. הסר מידע עודף, כולל נתונים כלשהם שנשארו מיומני ביקורות ואירועים.
- **הכנת הדמות לשכפול** – לאחר שווידאת שהמחשב הוגדר בדיוק כנדרש, הכן את המערכת לשכפול. בצע זאת על ידי הפעלת Sysprep עם קובץ אופציונלי Sysprep.inf, המתואר בהמשך סעיף זה. לאחר ש-Sysprep סיים לפעול, המחשב יכבה אוטומטית או יורה שכעת ניתן לכבותו בבטחה.
- **שכפול ההתקנה** – בשלב זה הדיסק הקשיח של המחשב מוכן להפעלת איתור הכנס-הפעל, יצירת SID (מזהה אבטחה) ייחודי, והפעלת אשף ההתקנה המצומצם בפעם הבאה שהמערכת תופעל. לפני המשך לשלב ההתקנה הבא, המערכת משוכפלת על ידי שימוש בתוכנית שירות צד-שלישי כגון Ghost של Symantec או Drive Image Pro של PowerQuest. בפעם הבאה שיתבצע אתחול של Windows 2000 Server מדיסק זה, או מכל דיסק קשיח אחר ששוכפל מדמות זו, המערכת תאתר ותקדד את התקני הכנס-הפעל, תיצור SID ייחודי, ותפעיל את אשף ההתקנה המצומצם להשלמת ההתקנה וההגדרה במחשב היעד.

אזהרה לא ניתן לשכפל רכיבים התלויים ב-Active Directory Services. אין ליצור משתמשים מקומיים וקבוצות על שרת החבר, כיון ש-SID חדשים לא יוקצו לחשבונות משמשים וקבוצות אלה.

קבצי Sysprep

כדי להשתמש ב-Sysprep, הפעל את Sysprep.exe ידנית, או הגדר שתוכנית ההתקנה תפעיל את Sysprep.exe אוטומטית על ידי שימוש בקטע [GuiRunOnce] של קובץ התשובות. להפעלת Sysprep, הקבצים Sysprep.exe ו-Setupcl.exe חייבים להיות מותקנים בתיקיה Sysprep בשורש כונן מערכת ההפעלה (%systemdrive%\Sysprep). להתקנת הקבצים במקומות הנכונים באמצעות תוכנית ההתקנה, עליך להוסיף קבצים אלה לתיקיות ההפצה שלך תחת תת התיקיה \$OEM$\$1\Sysprep.

קבצי Sysprep מכינים את מערכת ההפעלה לשכפול ומפעילים את אשף ההתקנה המצומצם. ניתן להוסיף את קובץ התשובות האופציונלי, Sysprep.inf, לתיקיה Sysprep. Sysprep.inf כולל פרמטרים של ברירת מחדל שבהם ניתן להשתמש לאספקת תגובות אחידות כנדרש. דבר זה מצמצם את הדרישה לתגובות מהמשתמש, ובכך מצמצם את סיכויי השגיאה שלו. ניתן גם להתקין את Sysprep.inf על דיסקט שיוכנס לכונן הדיסקטים לאחר שתיעלם תיבת הדו-שיח של טעינת האתחול. בכך ניתן לספק יותר תגובות מותאמות ולהפחית עוד יותר את הצורך באתחול ראשוני על ידי משתמש הקצה. לאחר שאשף ההתקנה המצומצם השלים את המטלות שלו בהצלחה, המערכת תאתחל שוב פעם אחת אחרונה, התיקיה Sysprep על כל תכולתה תמחק, והמערכת תהיה מוכנה להתחברות המשתמש.

קבצי Sysprep מוגדרים בסעיפים הבאים :

Sysprep.exe - ל-Sysprep.exe יש שלושה פרמטרים אופציונליים, המתוארים בטבלה להלן.

פרמטר	תיאור
quiet-	מפעיל את Sysprep ללא הצגת הודעות על המסך.
nosidgen-	מפעיל את Sysprep ללא יצירה מחודשת של SID הנמצאים כבר במערכת. דבר זה שימושי אם אינך מתכוון לשכפל את המחשב עליו אתה מפעיל את Sysprep.
reboot-	מאתחל את המחשב אוטומטית לאחר ש-Sysprep מכבה אותו, ומונע את הצורך לחזור ולהפעיל את המחשב ידנית. בנוסף, פרמטר reboot- מכריח אתחול מערכת לאחר ששכפול הדיסק הסתיים כך שתוכנית ההתקנה המצומצמת (גרסת תוכנית ההתקנה כאשר יש דמות משוכפלת על הדיסק) תפעל אוטומטית. הפעם היחידה שתרצה להשתמש במתג זה יהיה כאשר אתה מבקר את הליך Sysprep ואתה רוצה לוודא שאשף ההתקנה המצומצמת פועל כיאות.

Sysprep.inf - קובץ Sysprep.inf הוא קובץ תשובות המשמש בהליך השכפול כדי לספק נתונים ייחודיים להגדרת כל אחד ממחשבי היעד. הוא משתמש בתחביר קובץ מסוג ini. ושמות מפתח זהים (למפתחות נתמכים) כמו קובץ התשובות של תוכנית ההתקנה (unattend.txt). יש להתקין את קובץ Sysprep.inf בתיקיה \%systemdrive%\Sysprep או על דיסקט. אם אתה משתמש בדיסקט, מייד לאחר אתחול המערכת ועם הופעת מסך טעינת אתחול, הכנס את הדיסקט לכונן; המערכת תחפש קובץ Sysprep.inf מעודכן בכונן הדיסקטים. שים לב שאם אינך כולל את Sysprep.inf בעת הפעלת Sysprep, אשף ההתקנה המצומצם יציג את כל תיבות הדו-שיח הרשומים בקטע האשף המצומצם כפי שהם מופיעים בהמשך שיעור זה.

אם אתה משתמש ב-Sysprep.inf בעת הרכבת מחשב ההורה ובעת הפעלת Sysprep, השתמש בשיטת הדיסקט לאספקת חלופה ל-Sysprep.inf. המיקומים המוגדרים עבור קבצי מערכת ההפעלה בעת ההתקנה המצומצמת, כגון OEMPnPDriversPath ו-InstallFilesPath, חייבים להישאר זהים עבור Sysprep.inf שבתיקיית ההפצה ועבור Sysprep.inf שעל הדיסקט.

הקוד הבא הוא דוגמה לקובץ Sysprep.inf:

```
[Unattended]
;Prompt the user to accept the End Use License Agreement (EULA).
OemSkipEula=No
;Use Sysprep's default and regenerate the page file for the system
;to accommodate potential differences in available RAM.
KeepPageFile=0
;Provide the location for additional language support files that
;may be needed in a global organization.
InstallFilesPath=%systemroot%\Sysprep\i386
[GuiUnattended]
;Specify a non-null administrator password.
;Any password supplied here will take effect only if the original source
;for the image (master computer) specified a null password.
;Otherwise, the password used on the master computer will be
;the password used on this computer. This can be changed only by
;logging on as Local Administrator and manually changing the password.
AdminPassword=ABC123
;Set the time zone
TimeZone=20
;Skip the Welcome screen when the system boots
OemSkipWelcome=1
;Do not skip the regional options dialog so that the user can indicate
;which regional options apply to her or him.
OemSkipRegional=No
[UserData]
;Prepopulate user information for the system
FullName="Authorized User"
OrgName="Organization Name"
ComputerName=XYZ_Computer1
[GuiRunOnce]
;Promote this computer to a Domain Controller on reboot
DCPromo
[Identification]
;Join the computer to the domain ITDOMAIN
JoinDomain=ITDOMAIN
[Networking]
;Bind the default protocols and services to the network card(s) used
;in this computer.
InstallDefaultComponents=Yes
```

תוכל לשנות את סיסמת ה-Administrator באמצעות Sysprep.inf, רק אם סיסמת ה-Administrator (מנהל) הנוכחית היא null (לא פעילה). דבר זה נכון גם אם תרצה לשנות את סיסמת המנהל באמצעות Sysprep GUI. למידע נוסף אודות קבצי התשובות ופקודות המשמשות עם Sysprep.inf, ראה נספח B.

Setupcl.exe - קובץ Setupcl.exe מעבד את Sysprep.inf להגדרת דפים עבור אשף ההתקנה המצומצם ומפעיל את אשף ההתקנה המצומצם.

הערה שילוב של Sysprep.exe **ו-**Setupcl.exe **יכול לשמש במקום כלי** Rollback.exe **ששימש בגרסאות קודמות של** Windows NT.

אשף ההתקנה המצומצם

אשף ההתקנה המצומצם מתחיל בפעם הראשונה שמחשב מאתחל מדיסק ששוכפל באמצעות כלי Sysprep. האשף אוסף את כל המידע הנוסף הנדרש להתאים את מחשב היעד. אם אינך משתמש ב-Sysprep.inf או אם תשאיר קטעים ריקים בקובץ, אשף ההתקנה המצומצם יציג מסכים עבורם לא סופקו תשובות ב-Sysprep.inf .

להלן המסכים שאשף ההתקנה המצומצם עשוי להציג:

- EULA.
- Regional Options (אפשרויות אזוריות).
- User name and company (שמות המשתמש והחברה שבבעלותם מותקנת המערכת).
- Computer name and administrator password (שם מחשב וסיסמת Administrator).
- Network Settings (הגדרות רשת).
- Server Licensing (רשיונות שרת).
- Time Zone Selection (בחירת אזור זמן).
- Finish/Restart (סיים/אתחל).

אם ברצונך לעקוף מסכים אלה, תוכל להגדיר מספר פרמטרים בקובץ Sysprep.inf. הטבלה הבאה מהווה רשימת פרמטרים אלה.

פרמטר	ערך
EULA	[Unattended] OemSkipEula=Yes
Regional Options	[RegionalSettings] LanguageGroup=1 Language=00000409
User name and company	[UserData] FullName="user Name" OrgName="Organization Name"
Computer name and administrator password	[UserData] ComputerName=W2B32504 [GuiUnattended] AdminPassword="password"
Network Settings	[Networking] InstallDefaultComponents=Yes
הגדרות TAPI	[TapiLocation] AreaCode=425
Time Zone Selection	OEMSkipRegional=1 TimeZone=20
Finnish/Restart	NA

כיון שתוכנית ההתקנה מאתרת הגדרות מיטביות עבור התקני תצוגה, מסך Display Settings (הגדרות תצוגה) אינו מוצג בעת ההתקנה או בעת שימוש באשף ההתקנה המצומצם.

תוכל להגדיר הגדרות תצוגה או בקובץ התשובות המשמש ליצירת מחשב ההורה או בקובץ Sysprep.inf שישמש במחשב היעד. אם הגדרות התצוגה נמצאות בקובץ התשובות המשמש במחשב האב, Sysprep ישמור הגדרות אלה אלא אם Sysprep.inf מכיל הגדרות שונות או מתאם וידיאו שונה או מסך מסוג שונה, הדורשים הגדרות שונות ממחשב האב.

על ידי שימוש בערך OemSkipEula=Yes, אתה מקבל על עצמך אחריות להסכמה לכל דרישות הרשיון שבתוך EULA עבור משתמש זה.

אם תפעיל את תוכנית ההתקנה מהרשת והנך מתכוון להשתמש ב-Sysprep, עליך להגדיר את מתאמי הרשת באופן שונה מזה המבוצע בעת השימוש באפשרות InstallDefaultComponents. עליך לספק את נתוני הרשת היחודיים בקובץ Sysprep.inf.

במידה ומעוניינים לעבוד עם DHCP עבור כל המתאמים, ומספיק להתקין את Microsoft TCP/IP ,Client for Microsoft Networks, ושיתוף קבצים ומדפסות עבור רשתות Microsoft בכל המתאמים, אין צורך בהגדרה נוספת כלשהי בקובץ Sysprep.inf.

הפעלת Sysprep

קיימות שתי דרכים להפעיל את תוכנית השירות Sysprep: ידנית ואוטומטית.

הפעלה ידנית של Sysprep

לאחר שתתקין את Windows 2000 Server, תוכל להשתמש ב-Sysprep להכנת ההעברה של מערכת ההפעלה למחשבים בעלי תצורה דומה. להפעלה ידנית של Sysprep, עליך להתקין תחילה את Windows 2000 Server, להגדיר את המערכת, ולהתקין את היישומים. עתה הפעל את Sysprep ללא המתג reboot-. לאחר שהמערכת תכבה, שכפל את דמות הכונן למחשבים האחרים בעלי תצורה דומה.

הערה תוכנית השירות Sysprep נמצאת ב-Deploy.cab הממוקם בספריה \Support\Tools\ בתקליטור ההתקנה של Windows 2000 Server.

כאשר משתמשים יפעילו את מחשביהם המשוכפלים לראשונה, אשף ההתקנה המצומצם יופעל ויאפשר למשתמשים לשנות ולהתאים את מערכת ההפעלה באופן אישי. תוכל גם להקצות מראש את כל או חלק מהפרמטרים של Sysprep על ידי שימוש ב-Sysprep.inf. התיקיה Sysprep (הכוללת את Sysprep.exe ו-Setupcl.exe) נמחקת אוטומטית לאחר שתוכנית ההתקנה המצומצמת של Sysprep מסיימת את פעולתה.

המידע להלן מהווה סקירה על אופן ההכנה של התקנת Windows 2000 Server לשכפול:

- **הכנת התיקיה של Sysprep** – יש להכין בכפוף לתיקיית השורש של המערכת (%SystemRoot%) תיקיה בשם Sysprep. העתק אליה את Sysprep.exe ו-Setupcl.exe, ואם נדרש, גם את קבצי Sysprep.inf.
- **הפעלת תוכנית השירות Sysprep** – יש להפעיל את תוכנית השירות משורת פקודה בתיקיה Sysprep. השתמש באחת מהפקודות הבאות:

```
Sysprep
Sysprep -reboot
Sysprep / <optional parameter>
Sysprep / <optional parameter> -reboot
Sysprep / <optional parameter 1>…/ <optional parameter X>
Sysprep / <optional parameter 1>…/ <optional parameter X>
-reboot
```

- **הפעלת Sysprep ללא המתג reboot** – כאשר מופיעה הודעה המורה לכבות את המחשב, בחר בפקודת Shut Down מתפריט Start. עתה ניתן להשתמש בתוכנית שירות צד-שלישי ליצירת דמות (Image) של ההתקנה.
- **הפעלת Sysprep עם המתג reboot** – המחשב מאתחל אוטומטית ואשף ההתקנה המצומצם מופעל. יש לענות למנחי האשף. בנוסף, ניתן לבקר (Audit) את המערכת ויישומים אחרים. עם סיום הביקורת, יש להפעיל את Sysprep שנית עם המתג reboot- בשורת הפקודה. כאשר מופיעה הודעה המורה על כיבוי המחשב, בחר בפקודה Shut Down מתפריט Start. עתה ניתן להשתמש בתוכנית שירות צד-שלישי ליצירת דמות של ההתקנה.

הערה ניתן להוסיף לתיקיה Sysprep קובץ בשם Cmdlines.txt, שיעובד על ידי תוכנית ההתקנה. קובץ זה יפעיל פקודות שלאחר-התקנה, כולל אלה הנדרשות להתקנת יישומים.

הפעלה אוטומטית של Sysprep

קטע [GuiRunOnce] של קובץ התשובות כולל פקודות לביצוע לאחר סיום ההתקנה. ניתן להשתמש בקטע [GuiRunOnce] ליצירת התקנה המשלימה את תוכנית ההתקנה, מתחברת למחשב אוטומטית, מפעילה את Sysprep ב-Quiet Mode, ואז מכבה את המחשב.

להפעלה אוטומטית של Sysprep, יש להוסיף את קבצי Sysprep לתיקיית ההפצה תחת OEM\$1\Sysprep. פעולה זו תבטיח שהקבצים מועתקים למקום הנכון בכונן מערכת ההפעלה. בנוסף, הפקודה האחרונה בקטע [GuiRunOnce] של קובץ התשובות צריכה להיות כדלקמן:

```
%systemdrive%\Sysprep\Sysprep.exe -quiet
```

אם נדרשים מספר אתחולים, יש להוסיף פקודה זו כפריט האחרון שיופעל בקטע [GuiRunOnce] האחרון המשמש בקטע זה.

אם המחשב מאפשר תמיכה מתקדמת בצריכת החשמל (**A**dvanced **P**ower **M**anagement - APM) או תומך ב-ACPI, Sysprep יכבה את המחשב אוטומטית עם סיום הליך זה.

שימוש ב-Sysprep להרחבת מחיצות בדיסק

Windows 2000 מאפשרת הרחבת מחיצה במצב GUI. יעילות חדשה זו מאפשרת יצירת דמויות (Images) בעלות אפשרות הרחבה, לניצול דיסקים קשיחים להם יותר שטח משיש לדיסק המקורי על מחשב האב, באופן מלא. בנוסף, היא מספקת אמצעי להקטנת גודל הדמות, על ידי כך שאינה דורשת שהדמות תנצל את מלוא שטח הדיסק. בדרך זו, שטח הדיסק הניתן לניצול הוא מירבי. כיון ש-Sysprep משתמשת במצב GUI, היא יכולה לנצל שמישות זו.

אם תוכנית השירות שברשותך ליצירת דמות הדיסק מאפשרת עריכת הדמות, תוכל למחוק את הקבצים Pagefile.sys, Setupapi.log, וקובץ Hyberfil.sys (אם קיים), כיון שקבצים אלה ייווצרו מחדש בעת הפעלת אשף ההתקנה המצומצם במחשב היעד. **אין** למחוק קבצים אלה במערכת הפעלה פעילה, כיון שזה עלול לגרום לפעולה לא תקינה של המערכת. ניתן למחוק קבצים אלה, אם בכלל, מהדמות בלבד.

להרחבת מחיצת דיסק בעת שימוש בתוכנית השירות ליצירת דמות של צד-שלישי התומך ב-NTFS, תחילה עליך להגדיר את המחיצה על מחשב ההורה לגודל המינימלי הנדרש להתקנת Windows 2000 Server, כולל כל הרכיבים והיישומים. דבר זה יסייע להפחית את דרישות הגודל הכוללות של הדמות. ניתן גם לשנות את קובץ התשובות המשמש ליצירת דמות-ההורה על ידי הכללת אפשרות FileSystem=ConvertNTFS בקטע [Unattend]. אין לכלול כאן את ExtendOemPartition, כיון שנדרש לשמור על גודל דמות קטן ככל הניתן. עתה תוכל להתקין את Windows 2000 Server במחשב ההורה וליצור דמות של הכונן. משם, עליך להתקין את הדמות על מחשב היעד בו גודל מחיצת מערכת ההפעלה זהה לזו של מחשב האב. לאחר שתאתחל את מחשב היעד, אשף ההתקנה המצומצם יתחיל לפעול והמחיצה תורחב כמעט מייד.

שימוש בשרת ניהול מערכת - SMS

SMS (**S**ystems **M**anagement **S**erver), שרת ניהול מערכת) משמש לביצוע שדרוגים מבוקרים של Windows 2000 Server עבור מערכות רבות, במיוחד אלה המרוחקות גיאוגרפית. שים לב ש-SMS משמש רק להתקנות במחשבים בהם הותקנה בעבר מערכת הפעלה ואשר מפעילים SMS Client Agent (סוכן לקוח SMS) האחראי לקבלת הוראות התקנת תוכנה. לפני שתשתמש ב-SMS לביצוע שדרוג, עליך להעריך את תשתית הרשת הקיימת שלך, כולל רוחב פס, חומרה והגבלות גיאוגרפיות. היתרון העיקרי לשימוש ב-SMS לשדרוג הוא שתוכל לשמור על שליטה מרכזית של הליך השדרוג. לדוגמה, תוכל לקבוע מתי יתרחשו שדרוגים (כגון בעת או לאחר הכשרה, לאחר בדיקת חומרה, ולאחר גיבוי נתוני משתמשים), איזה מחשבים ישודרגו, וכיצד תיישם מגבלות רשת.

SMS 2.0 כולל Package Definition Files (קבצי הגדרת מנות, עם סיומת sms.) המאפשרת ייבוא שגרות התקנה של Windows 2000 Server לתוך מערך SMS 2.0 Package And Program Settings (הגדרות מנות ותוכנות SMS 2.0). לאחר ייבוא הגדרת

המנות, ספק ל-SMS מקור נתונים עבור תקליטור התקנת Windows 2000 Server, או מיקום נגיש ברשת המכיל את קבצי ההפצה של Windows 2000 Server.

שימוש בתקליטור לאתחול

ניתן להשתמש בשיטת תקליטור האתחול להתקנת Windows 2000 Server על מחשב בעל BIOS התומך באתחול מתקליטור. שיטה זו יעילה עבור מחשבים באתרים מרוחקים שהתקשורת אליהם איטית ושאין להם גישה למחלקת מידע מקומית. שיטת תקליטור האתחול מפעילה את Winnt32.exe, המאפשר התקנה מהירה.

הערה ניתן להשתמש בשיטת תקליטור לאתחול רק עבור התקנות חדשות. עבור שדרוגים, עליך להפעיל את Winnt32.exe ממערכת ההפעלה הקיימת.

להבטחת גמישות מירבית להתקנת Windows 2000 Server, הכן את סדר האתחול ב-BIOS כדלקמן:

- ❖ **מתאם רשת** – עבור זיכרון לקריאה בלבד (ROM) תואם PXE, ניתן להשתמש באפשרות זו לתמיכה בהתקנת מערכת הפעלה משרת RIS.
- ❖ **תקליטור** – עבור התקנת מערכות הפעלה התומכת באתחול באמצעות תקליטור.
- ❖ **דיסק קשיח** – עבור Sysprep או Syspart שהוכן להתקנה מקומית של מערכת ההפעלה.
- ❖ **דיסקט** – להתקנות מבוססות דיסקט.

כדי להשתמש בתקליטור להתקנה אוטומטית לחלוטין של מערכת הפעלה, הקריטריונים הבאים חייבים להתממש:

- ❖ BIOS המחשב שלך חייב לתמוך בפורמט El Torito Bootable CD-ROM (ללא הדמיה).
- ❖ קובץ התשובות חייב לכלול קטע [Data] עם המפתחות המתאימים.
- ❖ שם קובץ התשובות חייב להיות Winnt.sif והוא חייב להיות על דיסקט.

המידע הבא מהווה סקירה על אופן ההתקנה של Windows 2000 Server באמצעות תקליטור לאתחול.

- ❖ **אתחול מערכת ההפעלה** – לאחר הכנסת תקליטור Windows 2000 Server לכונן התקליטורים, יש לאתחל את מערכת ההפעלה.
- ❖ **טעינת קובץ Winnt.sif** – לאחר שהמערכת אתחלה, יופיע מסך התקנה כחול במצב טקסט עבור התקנת Windows 2000. הכנס את הדיסקט המכיל את קובץ Winnt.sif לכונן הדיסקטים. לאחר שהמחשב קורא את כונן הדיסקטים, הוציא את הדיסקט. עתה תוכנית ההתקנה תפעל מכונן התקליטורים כמוגדר בקובץ winnt.sif.

הערה שיטת האתחול מהתקליטור דורשת שכל הקבצים הנדרשים **יהיו** על התקליטור. לא **ניתן** להשתמש בקבצי UDF (**U**niqueness **D**atabase **F**iles) בשיטה **זו**. UDF אינם שמישים **כיון** שמזהה **ייחודי** נקרא עבור כל התקנה בעת **ציון** קובץ UDF מ-Winnt.exe **או** Winnt32.exe.

סיכום שיעור

קיימות ארבע שיטות לביצוע התקנה אוטומטית של Windows 2000 Server. השיטה הראשונה היא הפעלת פקודת Winnt32.exe יחד עם פרמטר Syspart. זוהי השיטה הנדרשת אם החומרה של מחשב היעד אינה דומה לחומרה של מחשב האב. אם החומרה דומה, תוכל להשתמש בתוכנית השירות Sysprep לביצוע התקנה אוטומטית. Sysprep הוא כלי המסייע ביצירת דמות הדיסק של ההתקנה שלך של Windows 2000 Server. אפשרות שלישית לביצוע התקנה אוטומטית היא להשתמש ב-SMS לביצוע שדרוג מבוקר ל- Windows 2000 Server עבור הרבה מערכות הפעלה, במיוחד לאלה המרוחקים גיאוגרפית. SMS משמש רק להתקנה במחשבים שבהם כבר מותקנת מערכת הפעלה קודמת וסוכן SMS מתאים. לבסוף, שיטה נוספת להתקנה אוטומטית היא באמצעות תקליטור אתחול. שיטה זו יעילה עבור מחשבים באתרים מרוחקים להם תקשורת איטית ואין להם מחלקת שירות.

שיעור 3: יצירת מערך אוטומטי להתקנת יישומי שרת

בנוסף ליצירת מערך להתקנה אוטומטית של מערכת ההפעלה Windows 2000 Server, תוכל להתקין גם יישומים אחרים במחשבי היעד באופן אוטומטי. יש שתי שיטות להתקנה אוטומטית של יישומי שרת: ניתן להשתמש בקובץ Cmdlines.txt או בקובץ התשובות. קובץ Cmdlines.txt כולל רשימת פקודות המתבצעות בשלב מצב GUI של התקנת Windows 2000. קובץ התשובות, המאפשר הפעלת התקנה אוטומטית של Windows 2000 Server, כולל את קטע [GuiRunOnce]. ניתן להוסיף תוכנית התקנת יישום או קובץ אצווה לקטע זה לצורך התקנה אוטומטית של יישומי שרת.

לאחר שיעור זה, תוכל

- להשתמש ב- Cmdlines.txt לביצוע התקנה אוטומטית של יישומי שרת.
- להשתמש בקטע [GuiRunOnce] של קובץ התשובות לביצוע התקנה אוטומטית של יישומי שרת.

זמן לימוד משוער: 45 דקות

שימוש בקובץ Cmdlines.txt

קובץ Cmdlines.txt מכיל את הפקודות המתבצעות בשלב GUI Mode של הליך ההתקנה. תוכנית ההתקנה מבצעת פקודות אלה בעת התקנת רכיבים אופציונליים, כגון יישומים שיש להתקין מייד אחרי התקנת Windows 2000 Server. אם אתה מתכוון להשתמש ב-Cmdlines.txt , יש להתקין את הקובץ בתת התיקיה \$OEM$ של תיקיית ההפצה. אם אתה משתמש ב-Sysprep, התקן את Cmdlines.txt בתת תיקיה \$OEM$\$1\Sysprep\.

יש להשתמש בקובץ Cmdlines.txt בנסיבות הבאות:

- בעת התקנת רכיבים מתת התיקיה \OEM של תיקיות ההפצה.
- כאשר היישום שאתה מתקין אינו מגדיר את עצמו לשימוש לריבוי משתמשים, כגון Microsoft Office 95, או שהוא מתוכנן להתקנה על ידי משתמש אחד ולשכפל מידע ייעודי-משתמש.
- כאשר אתה רוצה להתחבר כשירות ואתה רוצה שהשינויים שלך ישוכפלו אצל כל המשתמשים.

תחביר קובץ Cmdlines.txt הוא כדלקמן:

```
[Commands]
"<command_1>"
"<command_2>"
      .
      .
"<command_x>"
```

הפרמטרים **<command_1>**, **<command_2>** ו- **<command_x>** הם שומרי מקום עבור הפקודות שאתה רוצה להפעיל, לפי הסדר שאתה רוצה להפעילן כאשר תוכנית ההתקנה במצב GUI והיא קוראת לקובץ Cmdlines.txt . שים לב שכל הפקודות חייבות להופיע בין מרכאות.

קובץ Cmdlines.txt פועל כשירות, ולא כמשתמש מחובר בעל יכולות רשת. לכן, מידע ייחודי-משתמש נכתב לאוגר ברירת המחדל וכל המשתמשים הבאים בתור מקבלים גם הם מידע זה. בנוסף, Cmdlines.txt דורש שהקבצים הנדרשים להפעלת יישום או תוכנית שירות יהיו בתיקיות ההפצה.

שימוש בקובץ התשובות

קטע [GuiRunOnce] של קובץ התשובות כולל רשימת פקודות המבוצעות בפעם הראשונה שמשתמש מתחבר למחשב לאחר התקנה. לדוגמה, היית מוסיף את הפקודה הבאה לקטע [GuiRunOnce] כדי להפעיל את Sysprep באופן אוטומטי במצב Quiet:

```
[GuiRunOnce]
Command()="%systemdrive%\Sysprep\Sysprep -quiet"
```

הערה עליך להפעיל את Sysprep מ-[GuiRunOnce] כדי לשכפל הגדרות אצל כל המשתמשים.

יכולת חדשה של [GuiRunOnce] היא שימוש במשתנים סביבתיים, כפי שמתואר בדוגמה הקודמת. נתיבים מלאים פועלים אף הם.

בעת שימוש ב-[GuiRunOnce] ליזום התקנה, היה מודע, שאם היישום מאלץ אתחול מחדש, יש לבטל את האתחול. דבר זה חשוב, שכן כל פעם שהמערכת מאתחלת, כל נתוני RunOnce הקודמים הולכים לאיבוד. אם המערכת מבצעת אתחול לפני השלמת נתונים שנרשמו קודם בקטע RunOnce, הפריטים הבאים לא יפעלו.

אם אין שום אמצעי ביישום לביטול האתחול, תוכל לנסות לארוז את היישום מחדש במארז התקנה MSI או SMS. תוכנת VERITAS WinINSTALL LE כלולה ב-Windows 2000 Server, ו- SMS Installer כלול ב- SMS 2.0.

חלופה אחרת היא להכניס פקודה או כלי או יישום המאלץ אתחול חוזר בסיום מערך פקודות RunOnce. דבר זה דורש גם שלפני האתחול החוזר תוסיף פקודות RunOnce נוספות לרישום המערכת (Registry), כך שלאחר אתחול חוזר תעבד Windows 2000 את סדרת הפקודות הבאה. אפשר שהפקודה הראשונה ש-RunOnce תבצע תהיה פקודת עריכה של הרישום:

regedit /s <*filename.reg*>

שומר מקום **<filename.reg>** הוא קובץ רישום שניתן לו שם, או שקודד כנדרש לצורך ביצוע כל המטלות הנדרשות בעת שמתרחשים אתחולים חוזרים רבים. אם נדרשים אתחולים חוזרים רבים, כל קובץ **<filename.reg>** צריך להכיל, כפריט ראשון, פקודה לטעינת סדרת נתוני הרישום של RunOnce הבאים, עד שערכת הנתונים האחרונה מתבצעת.

תוכל להגדיר את הפרמטר AutoAdminLogonCount להתחבר באופן אוטומטי כ-Administrator למחשב. התחברות אוטומטית תומכת באתחולים רבים העלולים להיות נדרשים (נתמכים עד 99 אתחולים חוזרים). בנוסף, סיסמת מנהל מקומי (AdminPassword) חייבת להיכלל בקובץ התשובות המשמש להתקנת Windows 2000.

הערה אם אתה מתקין יישום עבור מספר גרסאות מקומיות (Localized) של Windows 2000, מומלץ לבחון את היישום שנארז מחדש בגירסה המקומית, כדי לוודא שהוא מעתיק קבצים למקומות הנכונים וכותב נתוני רישום כנדרש.

אם היישום דורש Microsoft Windows Explorer Shell לצורך התקנה, לא ניתן להשתמש בקטע [GuiRunOnce] כיון שה-Shell (מעטפת) לא תיטען בעת שפקודות Run ו-RunOnce מבוצעות. בדוק עם ספקי היישום אם יש להם עדכון או קובץ תיקון (Patch) המטפל בכך לצורך התקנת היישום. אם לא, תוכל לארוז את היישום מחדש במארז MSI או להשתמש באמצעי הפצה אחרים.

יישומים המשתמשים במנגנוני התקנה מאותו סוג, עלולים שלא לפעול כנדרש אם לא תשתמש בפקודה wait/ (המתן). דבר זה קורה בעת שהתקנת יישום פועלת, ובו בזמן מתחיל הליך נוסף. אף ששגרת ההתקנה עדיין פועלת, על ידי יזום הליך אחר וסגירת הליך פעיל, ייתכן שהשגרה הבאה הרשומה במפתח RunOnce ברישום תתחיל לפעול. כיון שיותר מאירוע התקנה אחד פעיל, היישום השני ייכשל.

התקנת יישומים

ניתן להשתמש בשתי שיטות להתקנת יישומים באמצעות קטע [GuiRunOnce] של קובץ התשובות: שימוש בתוכניות להתקנת יישומים ושימוש בקבצי אצווה.

שימוש בתוכניות להתקנת יישומים

השיטה המועדפת להתקנה מראש של יישום היא שימוש בתוכנית ההתקנה המסופקת עם היישום. ניתן לעשות כן אם היישום שאתה מתקין מסוגל לפעול במצב שקט (Quiet) (ללא התערבות המשתמש). מצב שקט לרוב דורש מתג שורת פקודה q/ או s/. עיין בתיעוד היישום או קובץ העזרה שלו לרשימת פרמטרים עבור שורת הפקודה הנתמכים על ידי מנגנון ההתקנה.

הפקודה הבאה היא דוגמה לשורה שתוכל לכתוב בקטע [GuiRunOnce] ליזום התקנה אוטומטית של יישום. שים לב שפקודה זו משתמשת בתוכנית ההתקנה של עצמה:

```
<path to setup>\Setup.exe /q
```

פרמטרים של התקנה משתנים בין יישומים. לדוגמה, בפרמטר I/, הכלול במספר יישומים, ניתן להשתמש כאשר יש ליצור קובץ יומן לבקרת ההתקנה. לחלק מהיישומים יש פקודה המונעת ממנו לאתחל באופן אוטומטי. דבר זה יעיל בבקרה של התקנת יישומים עם מספר מזערי של אתחולים.

בדוק עם ספק היישום לקבלת מידע, הוראות, כלים ונהלים רצויים לפני התקנת היישום.

הערה עליך לעמוד בתנאי הרשיון של כל יישום שתתקין, בלי שום קשר לשיטת ההתקנה.

שימוש בקובץ אצווה לשליטה על אופן ההתקנה של יישומים רבים

אם ברצונך לשלוט על התקנת מספר יישומים רב, תוכל ליצור קובץ אצווה המכיל פקודות התקנה ייחודיות ומשתמש בפקודת Start של Windows 2000, יחד עם מתג שורת הפקודה Wait/. ניתן להפעיל את קובץ האצווה מקטע [GuiRunOnce] של קובץ התשובות. השימוש בקובץ אצווה מבטיח שכל יישום מותקן לפי סדר ובמלואו לפני שמתחילה שגרת ההתקנה של היישום הבא.

המידע הבא מהווה סקירה על אופן יצירת קובץ אצווה, התקנת היישום, והסרת כל התייחסות לקובץ האצווה לאחר השלמת ההתקנה:

- **יצירת קובץ האצווה** – על קובץ האצווה להכיל שורות פקודה, בדומה לדוגמה הבאה:

```
Start /wait <path>\<setup file> <command line parameters>
Start /wait <path>\<setup file> <command line parameters>
Exit
```

כאשר:

שומר מקום **<path>** הוא הנתיב לקבצי ההפעלה המתחילים את ההתקנה. נתיב זה חייב להיות זמין בעת ההתקנה.

שומר מקום **<setup file>** הוא שם קובץ ההפעלה המתחיל את ההתקנה.

שומרי מקום **<command line parameters>** הם פרמטרים מצב-שקט כלשהם המתאימים ליישום שנדרש להתקין.

- **העתקת קובץ האצווה** – יש להעתיק את קובץ האצווה לתיקיית ההפצה או כל מקום אחר הנגיש בעת ההתקנה. אם בכוונתך להפעיל את Sysprep במחשב עליו אתה מתקין את Windows 2000, ניתן להעתיק את קובץ האצווה לתיקיה Sysprep של תיקיות ההפצה. דבר זה יהפוך את קובץ האצווה למקומי עבור המחשב המותקן. כאשר מפעילים את המחשב לאחר שקובץ Sysprep הופעל ותוכנית ההתקנה המצומצמת הסתיימה, התיקיה Sysprep על כל תכולתה תמחק. אין צורך למחוק את קובץ האצווה בדרך אחרת.

- **הוספת קובץ האצווה לקובץ התשובות** – יש להוסיף רישום עבור קובץ האצווה בקטע [GuiRunOnce] של קובץ התשובות.

- **העתקת קובץ ink. למחשב המקור** – יש להעתיק קובץ ink ממחשב המקור לתיקיה

OEM\$1\documents and settings\all users\stasrt menu\programs\startup

כאשר המחשב מתחיל לפעול שנית, ועובד במצב GUI, מותקן היישום והקובץ ink נמחק מקבוצת ההתחלה (Startup Group).

סיכום שיעור

ניתן להשתמש בשתי שיטות להתקנה אוטומטית של יישומי שרת. הראשונה היא שימוש בקובץ Cmdlines.txt, המכיל פקודות המופעלות בשלב GUI Mode של תהליך ההתקנה. תוכנית ההתקנה מבצעת פקודות אלו בעת התקנת רכיבים אופציונליים. השיטה השניה היא לשנות את קטע [GuiRunOnce] של קובץ התשובות. קטע זה מכיל רשימת פקודות המתבצעות בפעם הראשונה שמשתמש מתחבר לאחר שתוכנית ההתקנה סיימה. אם ברצונך להשתמש בקובץ התשובות להתקנת יישומים, תוכל להשתמש בשגרת ההתקנה המצורפת ליישום, או שתוכל ליצור קובץ אצווה ובו פקודות ההתקנה הייחודיות.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות לשאלה, עיין בשיעור המתאים ונסה את השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואח״כ בעברית.

The following questions are intended to reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A.

1. What is the purpose of using the / tempdrive: or / t: installation switches with Winnt32. exe or Winnt. exe, respectively?
2. You are asked to develop a strategy for rapidly installing Windows 2000 Server for one of your clients. You have assessed their environment and have determined that the following three categories of computers require Windows 2000 Server:
   - There are 30 unidentical computerconfigurations currently running Windows NT Server 4.0 that need to be upgraded to Windows 2000 Server.
   - There are 20 identical computers that need a new installation of Windows 2000 Server.
   - Remote sites will run a clean installation of Windows 2000 Server. You want to make sure that they install a standard image of Windows 2000 Server that is consistent with your local configuration of the operating system. You will provide them with hard disks that they will install in their servers.

   What are the steps for your installation strategy?
3. What is the purpose of the $ OEM$ folder and the subfolders created beneath it by Setup Manager?
4. How does Cmdlines. txt differ from [GuiRunOnce]?
5. How does Syspart differ from Sysprep?

1. מה הסיבה לשימוש במתגי ההתקנה :tempdrive/ או :t/ עם Winnt32.exe או Winnt.exe בהתאמה?

2. אתה נדרש לפתח מערך התקנה מהיר להתקנת Windows 2000 Server עבור אחד מלקוחותיך. בחנת את סביבת העבודה שלו וקבעת ששלוש קטגוריות המחשבים הבאות דורשות Windows 2000 Server:

   - ישנן 30 תצורות מחשב לא זהות המפעילות כרגע Windows NT Server 4.0, שיש לשדרג אותן ל-Windows 2000 Server.
   - ישנן 20 התקנות זהות שבהן נדרשת התקנה חדשה של Windows 2000 Server.
   - אתרים מרוחקים יפעילו התקנה חדשה של Windows 2000 Server. ברצונך לוודא שהם יתקינו דמות סטנדרטית של Windows 2000 Server התואמת את התצורה המקומית של מערכת ההפעלה. אתה תספק להם דיסקים קשיחים שהם יתקינו בשרתים שלהם.

   מה הם השלבים הנדרשים ליישום אסטרטגיית ההתקנה שלך?

3. מה מטרת התיקיה OEM ותת התיקיות מתחתיה הנבנות על ידי Setup Manager (מנהל ההתקנה)?

4. במה שונה Cmdlines.txt מ-[GuiRunOnce]?

5. במה שונה Syspart מ-Sysprep?

פרק 4

מערכת הקבצים של Windows 2000

אודות פרק זה

Windows 2000 תומכת NTFS ‏(NT File System) ושתי שיטות של File Allocation : FAT16 ו- FAT32, עבור קריאה וכתיבת נתונים. תמיכה לקריאה בלבד מסופקת על ידי CD-ROM file system ‏(CDFS), מערכת קבצים עבור תקליטורים) ו-**U**niversal **D**isk **F**ormat ‏(UDF, פורמט דיסקים אוניברסלי). פרק זה מתמקד בשיטת הקבצים הניתנת לכתיבה של Windows 2000.

מבנה ה-Volumes וארגון הקבצים בשיטת NTFS שונה באופן משמעותי מ-FAT. גרסת NTFS 5.0, שהיא גרסת NTFS המשמשת ב-Windows 2000, כוללת מספר תכונות התומכות בתפקודיות החדשה של Windows 2000, תפקודיות שאינה נתמכת על ידי FAT ורק חלקית על ידי NTFS במערכת הפעלה Windows NT 4.0. פרק זה מהווה מבוא בסיסי לניהול דיסקים, וממשיך ומתאר את FAT ו-NTFS. בנוסף, פרק זה גם דן באבטחת תיקיות וקבצים וכיצד היא מיושמת בסביבת FAT ו-NTFS.

לפני שתתחיל

לביצוע השעורים בפרק זה, נדרש שיהיו ברשותך ציוד ותוכנות כדלקמן:

- עמידה בדרישות המפורטות בפרק ההקדמה כך ש- Server01 יהיה בעל 500MB שטח דיסק בלתי מוקצה (ללא מחיצה) בדיסק הראשון (Disk0).
- השלמת התרגילים בפרק 2 ופרק 3 כך ששני המחשבים מפעילים Windows 2000 Server והם בתצורה המפורטת בתרגילים.

שיעור 1 : ניהול דיסקים בסיסי

לפני שתוכל להתקין את Windows 2000 Server על דיסק קשיח, יש להגדיר את אותו חלק בדיסק שישמש את Windows 2000, בסוג האחסון, המחיצה והפרמוט. אם מחיצות המערכת (System Partition) ומחיצת האתחול (Boot Partition) יהיו נפרדות, יש לחלק למחיצות ולפרמט גם את שטח הדיסק המכיל את קבצי המערכת וגם את שטח הדיסק המכיל את קבצי האתחול של מערכת ההפעלה. שיעור זה מהווה סקירה על דרך הגדרת מדיה לאחסון ומספק מידע אודות מטלות תחזוקת דיסקים.

לאחר שיעור זה, תוכל

- לתאר תפיסות בניהול דיסקים.
- לזהות מטלות ניהול דיסקים נפוצות.
- ליצור ולהגדיר דיסק דינמי.

זמן לימוד משוער: 60 דקות

הגדרת דיסק קשיח

בין אם אתה מגדיר את השטח הפנוי שנותר על הדיסק לאחר התקנת Windows 2000 או שאתה מגדיר דיסק חדש, קיימות מספר מטלות שיש לבצע להכנת הדיסק.

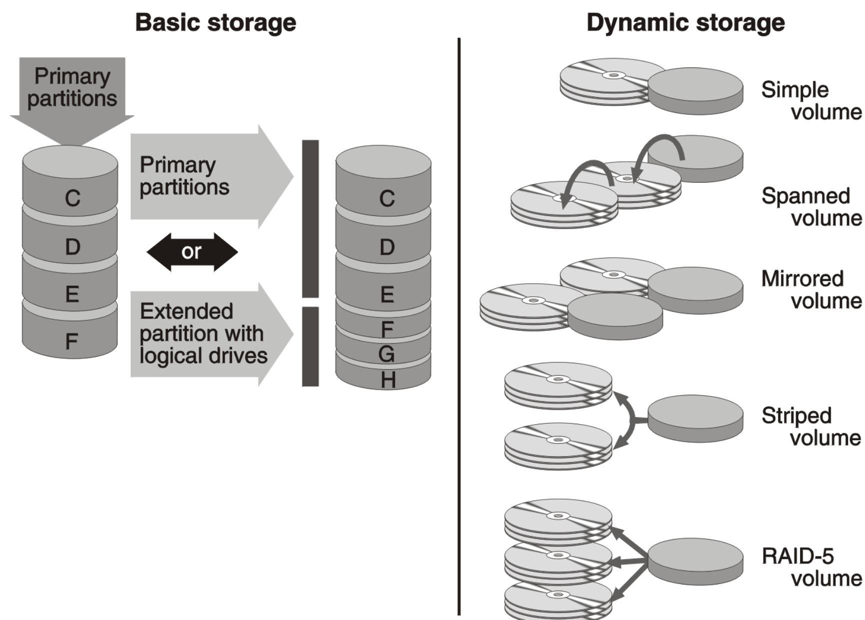
- **יש לאתחל את הדיסק עם סוג האחסון** – האתחול מגדיר את המבנה הבסיסי של הדיסק. Windows 2000 תומכת בשני סוגים של מבנה אחסון נתונים בדיסקים: Basic Storage (אחסון בסיסי) ו-Dynamic Storage (אחסון דינמי).
- **יצירת Patritions או Volumes** – עליך ליצור מחיצות (Patritions) על דיסק בסיסי או Volumes על דיסק דינמי.
- **פרמוט דיסק** – לאחר שיצרת מחיצה או Volume, עליך לפרמט אותה בשיטת קבצים ייחודית – NTFS, או אחד משני הסוגים של מערכת קבצים FAT16: FAT או FAT32. שיטת הקבצים בה תשתמש תשפיע על פעולות הדיסק. זה כולל שליטה על גישת משתמשים למידע, אחסון נתונים, נפח הדיסק הקשיח, ואיזו מערכת הפעלה יכולה לגשת לנתונים שעל הדיסק הקשיח.

אחסון, Partitions and Volumes

לפני שתחליט כיצד לבצע את המטלות להגדרת דיסק קשיח, עליך להתמצא בסוגי האחסון, סוגי המחיצות וסוגי ה-Volumes הזמינים במערכת Windows 2000.

סוגי אחסון

מערכת Windows 2000 תומכת בשני סוגים של מבנה אחסון נתונים בדיסקים: אחסון בסיסי ואחסון דינמי. דיסק פיסי חייב להיות או בסיסי או דינמי; לא ניתן להשתמש בשני הסוגים של אחסון באותו דיסק. אולם, תוכל להשתמש בשני הסוגים של האחסון במערכת רב-דיסקים, כמתואר בתרשים 4.1.



תרשים 4.1 אחסון בסיסי ודינמי.

הערה סוגי האחסון של Windows 2000 נבדלים מתצורות אשכול דיסקים ברמת-החומרה. אשכול דיסקים ידוע יותר כ- **D**isks **I**ndependent Of **A**rray **R**edundant (RAID, מערך דיסקים עצמאיים). RAID ברמת-החומרה נראה ל-Windows 2000 כשטח בלתי-מוקצה. שטח זה מוגדר על ידי Windows 2000 כשטח אחסון בסיסי או דינמי.

Basic Storage

התקן התעשייתי המסורתי הוא Basic Storage (אחסון בסיסי). הוא מכתיב חלוקת דיסק קשיח למחיצות. **מחיצה** (Partition) היא חלק מהדיסק המתפקדת כיחידת אחסון פיסית עצמאית. Windows 2000 מכירה במחיצות ראשיות (Primary Partitions) ומורחבות (Extended Partitions). דיסק המאתחל עבור אחסון בסיסי נקרא **דיסק בסיסי** (Basic Disk). דיסק בסיסי יכול להכיל מחיצות ראשיות, מחיצות מורחבות, וכוננים לוגיים. דיסקים חדשים הנוספים למחשב המפעיל Windows 2000 הם דיסקים בסיסיים.

כיון שאחסון בסיסי הוא הסטנדרט התעשייתי הבסיסי, מערכות הפעלה MS-DOS, כל הגרסאות של Windows (9x/NT/2000) תומכות באחסון בסיסי. עבור Windows 2000 אחסון בסיסי הוא ברירת המחדל, כך שכל הדיסקים הם דיסקים בסיסיים עד שתסב אותם לאחסון דינמי.

דיסק בסיסי תואם לאחור עם סט מחיצות של Windows NT, Volume Sets, Striped Sets (RAID-0), Mirror Volumes (RAID-1), ו- Disk Striping With Parity (RAID-5).

Dynamic Storage

רק Windows 2000 תומכת ב-Dynamic Storage (אחסון דינמי). לתמיכה באחסון דינמי, יוצרים Volume בודד הכולל את הדיסק כולו. דיסק המאתחל עבור אחסון דינמי הוא **דיסק דינמי**.

דיסקים דינמיים מחולקים ל- Volumes, העשויים להכיל חלק או חלקים של דיסק פיסי אחד או יותר. דיסק דינמי יכול להכיל:

- Simple Volumes (כרכים פשוטים),
- Spanned Volumes,
- Striped Volumes (RAID-0),
- Mirrored Volumes (RAID-1),
- Striped with parity Volumes (RAID-5).

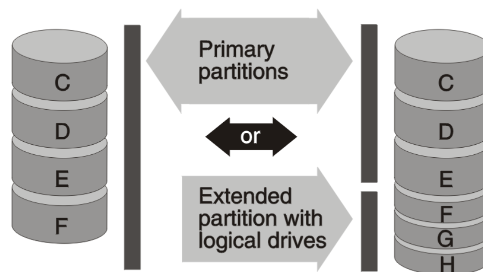
אתה יוצר דיסק דינמי על ידי שדרוג דיסק בסיסי.

לאחסון דינמי אין את המגבלות שיש לאחסון בסיסי; לדוגמה, תוכל להגדיר ולשנות מימדי דיסק דינמי, מבלי לאתחל את Windows 2000 מחדש.

הערה התקני **אחסון** ניידים מכילים מחיצות ראשוניות (Primary Partition) בלבד. לא תוכל ליצור מחיצות מורחבות, כוננים לוגיים, או Dynamic Volumes על התקני **אחסון** ניידים. לא תוכל לסמן מחיצה ראשית על התקן **אחסון** נייד כפעילה.

סוגי מחיצות בדיסק בסיסי (Basic Disks)

ניתן לחלק דיסק בסיסי למחיצות ראשיות (Primary) ומורחבות (Extended). מחיצה מתפקדת כיחידת אחסון פיסית נפרדת. כך מתאפשרת הפרדה בין סוגי מידע שונים, כגון נתוני משתמש במחיצה אחת ויישומים בשנייה. Basic Disk (דיסק בסיסי) יכול להכיל עד ארבע מחיצות ראשיות, או עד שלוש מחיצות ראשיות ומחיצה מורחבת אחת, ובסך הכל ארבע מחיצות. רק מחיצה אחת יכולה להיות מחיצה מורחבת, כמתואר בתרשים 4.2.



תרשים 4.2 סוגי מחיצות.

Primary Partitions

Windows 2000 משתמשת ב-Primary Partitions (מחיצות ראשיות) להפעלת המחשב. אחת מהמחיצות הראשיות האלה מסומנת כמחיצה פעילה. **מחיצה פעילה** (Active Partition) היא המקום בו החומרה מחפשת את קבצי האתחול של מערכת ההפעלה. רק מחיצה אחת על דיסק קשיח בודד יכולה להיות פעילה בכל רגע נתון. קיום מספר מחיצות ראשיות מאפשר בידוד מערכות הפעלה שונות או סוגי נתונים. לאתחול כפול של Windows 2000 עם Windows 95 או MS-DOS, יש לפרמט את המחיצה הפעילה בתצורת FAT16, כיון שמערכת Windows 95 אינה יכולה לקרוא מחיצה בתצורת FAT32 או NTFS. לאתחול כפול עם Windows 95 OSR2 (גירסה מאוחרת של Windows 95 שכללה שיפורים, כגון היכולת לקרוא מחיצות בתצורת FAT32), או עם Windows 98, יש לפרמט את המחיצה הפעילה כ-FAT16 או FAT32.

הערה ככל הידוע, Windows 95 בגרסת OSR2 לא הופצה מעולם מחוץ לארה"ב. ההתייחסות לגירסה זו בספר נובעת רק משיקולי תאימות לבחינות ההסמכה.

טיפ אם המחיצה הפעילה מפורמטת עם NTFS, ניתן להתחיל את Windows 9X מדיסקט. הדיסקט מכיל מציין למחיצת FAT המכילה את Windows 9X.

מחיצת המערכת (System Partition) של Windows 2000 (מכונה גם System Volume, בתיעוד Windows 2000), היא המחיצה הפעילה הכוללת קבצים ייחודים-חומרה לטעינת מערכת ההפעלה. **מחיצת האתחול** (Boot Partition) של Windows 2000 היא

המחיצה הראשית או הכונן הלוגי בו מותקנים קבצי מערכת ההפעלה. מחיצת האתחול ומחיצת המערכת יכולים להיות אותה מחיצה. אולם, מחיצת המערכת חייבת להיות על המחיצה הפעילה, לרוב כונן C, בעוד שמחיצת האתחול יכולה להיות על מחיצה ראשית אחרת או על מחיצה מורחבת.

Extended Partitions

מחיצה מורחבת (Extended Partition) נוצרת מאזור דיסק פנוי. יכולה להיות רק מחיצה מורחבת אחת על דיסק קשיח, כך שחשוב לכלול במחיצה המורחבת את כל השטח הפנוי שנותר לאחר חלוקת הדיסק למחיצות ראשיות. שלא כמו מחיצות ראשיות, אינך מפרמט מחיצות מורחבות ואינך מקצה להן אות כונן. מחיצות מורחבות מחולקות לקטעים. כל קטע הוא כונן לוגי. אתה מקצה אות לכל כונן לוגי, ומפרמט אותו באחת משיטות מערכות הקבצים.

סוגי Volumes בדיסק דינמי (Dynamic Disks)

תוכל לשדרג דיסקים בסיסיים לאחסון דינמי ואז ליצור Windows 2000 Volumes. שקול איזה סוג Volume מתאים ביותר לצרכיך לשימוש יעיל בשטח הדיסק, ביצועים, ו-Fault tolerance. **סיבולת תקלות** (Fault Tolerance) היא היכולת של מחשב או מערכת הפעלה להיענות לאירוע אסון, ללא איבוד נתונים. ב-Windows 2000, ל-Volume מסוג RAID-1 ו- RAID-5, יש Fault tolerance.

Simple Volume

Simple Volume מכיל שטח דיסק מדיסק בודד ואין לו Fault tolerance. ניתן להרחיב Simple Volumes לרב-אזוריים (עד 32 אזורים) באותו דיסק. Simple Volumes אינם מספקים Fault tolerance. למעשה, הם בעלי סיבולת תקלות נמוכה יותר מאשר Spanned Volumes, כיון שהרחבת Simple Volume מגדילה את מספר נקודות הכשל בדיסק.

Spanned Volume

Spanned Volume הוא שטח דיסק המורכב ממספר דיסקים (2-32). Windows 2000 כותבת נתונים ל-Spanned Volume על ידי כתיבה לדיסק הראשון, תוך מילוי כל שטחו, וממשיכה בדרך זו בכל דיסק המהווה חלק מה-Spanned Volume. ל-Spanned Volume אין Fault tolerance. אם דיסק כלשהו ב-Spanned Volume נכשל, הנתונים בכל ה-Volume אובדים.

Mirrored Volume

Mirrored Volume מורכב משני העתקים זהים של Simple Volume, כל אחד על דיסק נפרד. ל-Mirrored Volumes יש Fault tolerance במקרה של כשל דיסק.

Striped Volume

Striped Volume (RAID-0), משלב שטח דיסק פנוי מדיסקים רבים (מ-2 עד 32 דיסקים) ל-logical volume אחד. Windows 2000 משפרת ביצועים על ידי הוספת נתונים לכל הדיסקים באותו קצב. אם דיסק ב-Striped Volume כשל, כל ה-Volume אובד. אי לכך, כמו בהרחבת Simple Volume או יצירת Spanned Volume, ל-RAID-0 אין Fault tolerance, אבל הוא נותן מהירות קריאה גדולה יותר.

RAID-5 Volume

RAID-5 Volume הוא Striped Volume בעל Fault tolerance. Windows 2000 מוסיפה Parity Information Strip לכל מחיצת דיסק ב-Volume. Windows 2000 משתמשת ב-Parity Information Strip לשחזור נתונים, במידה ודיסק פיסי כשל. ליצירת Volume RAID-5 נדרשים לפחות 3 דיסקים ועד 32 דיסקים.

מגבלות Dynamic Disk ו-Dynamic Volume

רק מערכות המריצות Windows 2000 מסוגלות לקרוא דיסקים דינמיים. כך, לא תוכל להשתמש בדיסקים דינמיים אם ברצונך לבצע אתחול כפול של מערכת הפעלה אחרת הדורשת גישה לדיסקים בעלי תצורת אחסון דינמית. Dynamic Volumes אינם נתמכים על ידי מחשבים ניידים מסוגים שונים. לא ניתן ליצור תצורת Fault tolerance (RAID-1 ו-RAID-5) באופן מקומי במחשבי Windows 2000 Professional.

מערכות קבצים

Windows 2000 תומכת בכתיבה וקריאה עבור מערכות קבצים NTFS, FAT16 ו-FAT32. אף שמחיצות NTFS ו-FAT תומכות בדיסקים בסיסיים ודינמיים, עליך להשתמש במחיצת NTFS כאשר נדרש שמחיצה תהיה מאובטחת ברמת הקובץ והתיקיה, תהיה לה יכולת דחיסת דיסק, מכסות דיסק או הצפנה. רק Windows 2000 ו-Windows NT יכולות לגשת לנתונים על דיסק מקומי המפורמט NTFS. אם אתה מתכנן לקדם שרת להיות Domain Controller (בקר תחום), פרמט את מחיצת ההתקנה עם NTFS. דבר זה נדרש עבור התמיכה ב-Active Directory Services.

FAT16 ו-FAT32 מאפשרות גישה על ידי מערכות הפעלה אחרות ותאימות איתן. כדי לבצע אתחול כפול של Windows 2000 ומערכת הפעלה נוספת, פרמט את מחיצת מערכת ההפעלה עם FAT16 או FAT32. FAT אינה מציעה רבות מהתכונות הנתמכות על ידי NTFS, כגון אבטחה ברמת הקובץ. אי לכך, ברוב המצבים רצוי לפרמט את הדיסק

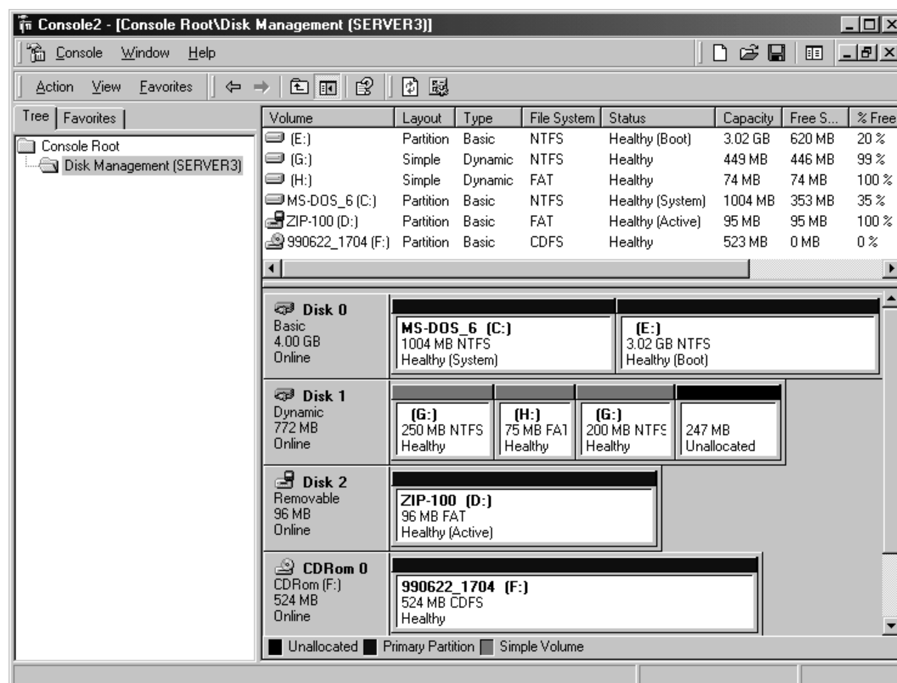
עם מערכת NTFS. הסיבה היחידה לשימוש ב-FAT16 או FAT32, היא עבור אתחול כפול. שיעורים 2 ו- 3 מספקים מידע נוסף אודות FAT ו-NTFS.

מטלות שכיחות לניהול דיסק

תוסף התוכנה לניהול דיסקים (Disk Management Snap-In) המוצג בתרשים 4.3, מרכז את המידע על הדיסק ומטלות ניהול, כגון יצירה ומחיקה של Partitions ו-Volumes. עם ההרשאות הנדרשות, תוכל לנהל דיסקים מקומיים ודיסקים על מחשבים מרוחקים.

תוכל ליצור MMC Console מותאם אישית ולהוסיף לו את תוסף התוכנה של ניהול הדיסק. תוסף התוכנה לניהול הדיסק נכלל גם ב-Preconfigured Management MMC שבתפריט Administrative Tools. תוסף התוכנה לניהול דיסקים מספק תפריטי קיצור-דרך המורים איזה מטלות ניתן לבצע על אובייקטים נבחרים, והוא כולל אשפים המדריכים אותך ליצירת partitions ו-volumes ושדרוג דיסקים.

השתמש בתוסף התוכנה לניהול דיסקים להגדיר ולנהל את שטח האחסון של הרשת. תוסף התוכנה לניהול דיסקים יכול להציג את מערכת האחסון בצורה גרפית או כרשימה. תוכל לשנות את התצוגה ולהתאימה לצרכיך באמצעות הפקודות בתפריט View.



תרשים 4.3 Disk Management Snap-in (ניהול דיסק).

בנוסף לניטור נתוני הדיסק, ייתכן שתצטרך לבצע מטלות ניהול דיסק נוספות, כולל הוספה והסרת דיסקים קשיחים ושינוי סוג האחסון של הדיסק. שדרוג דיסק בסיסי לדיסק דינמי מתואר בתרשים 4.4.

תרשים 4.4 שדרוג דיסק מאחסון בסיסי לדינמי.

עבודה עם Simple Volumes

Simple Volume כולל שטח דיסק בדיסק בודד. ניתן להרחיב Simple Volume כדי לכלול שטח לא מוקצה על אותו דיסק. ל-Simple Volume אין Fault tolerance; אולם, תוכל להגדיר שני Simple Volumes המהווים שיקוף (Mirrored, תמונת ראי) אחד לשני. תוכל לפרמט Simple Volume ב-NTFS, FAT16 או FAT32, אך ה-Volume ניתן להרחבה רק אם הוא מפורמט NTFS.

ניתן ליצור Simple Volume על ידי בחירת Disk Management בקטע האחסון של תוסף התוכנה של Computer Management. בדיסק הדינמי שבו ברצונך ליצור את ה-Volume, לחץ לחיצה ימנית על השטח הבלתי מוקצה ואז לחץ Create Volume. פעולה זו תפעיל את אשף Create Volume. האשף מוליך אותך דרך השלבים הנדרשים ליצירת Simple Volume.

להרחבת NTFS Simple Volume, לחץ לחיצה ימנית על ה-Simple Volume שברצונך להרחיב ולחץ Extend Volume. פעולה זו תפעיל את האשף. עקוב אחר ההוראות על המסך לשימוש בשטח לא מוקצה על דיסק דינמי כלשהו להרחבת ה-Volume הקיים. בעת הרחבת Simple Volume לדיסק אחר, הוא נהפך ל-Spanned Volume.

הערה Simple Volume בפורמט NTFS, **ניתן** להרחבה רק במידה **והוא נוצר** כ-Volume חדש על דיסק דינמי. במידה **וה**-Simple Volume **נוצר** בזמן ההסבה ממחיצה שהיתה על דיסק בסיסי, לא ניתן יהיה להרחיבו.

עבודה עם Spanned Volumes

Spanned Volumes מורכבים משטח דיסק מדיסקים רבים; Spanned Volumes מאפשרים שימוש יעיל יותר של סך כל השטח הבלתי מוקצה הקיים על דיסקים רבים. ניתן ליצור Spanned Volumes רק על דיסקים דינמיים, ונדרשים שני דיסקים דינמיים לפחות ליצירת Spanned Volume. Spanned Volumes אינם יכולים להוות חלק מ-Mirrored Volume או Striped Volumes ואין להם Fault tolerance.

חיבור שטח פנוי ליצירת Spanned Volume

ניתן ליצור Spanned Volume על ידי חיבור שטחים פנויים בגדלים שונים ב- 2 עד 32 דיסקים, ליצירת Logical Volume אחד גדול. שטחי הדיסק הפנויים המרכיבים את ה-Spanned Volume יכולים להיות בגדלים שונים. Windows 2000 מארגנת Spanned Volumes כך שהמידע מאוחסן על שטח של דיסק אחד עד שהוא מלא. אז, הנתונים מאוחסנים על הדיסק השני, מהתחלתו. Windows 2000 ממשיכה בדרך זו על כל דיסק נוסף עד למקסימום של 32 דיסקים.

על ידי מחיקת Volumes קטנים ומיזוגם ל-Spanned Volume אחד, ניתן לשחרר אותיות כוננים לצרכים אחרים וליצור Volume גדול עבור קבצי המערכת.

הערה ניתן להגדיר את כל תצורות הדיסק הדינמיות הזמינות במערכת Windows 2000 לשימוש בטכנולוגיות שונות, יצרנים שונים, או דגמי בקרים שונים במחשב. לדוגמה, דיסק דינמי אחד ב-Spanned Volume עשוי להיות מחובר לבקר (**I**ntegrated **D**evice **E**lectronics IDE), בעוד שדיסק אחר מחובר לבקר SCSI (**S**mall **C**omputer **S**ystem **I**nterface).

הרחבה ומחיקה של Spanned Volumes

ניתן להרחיב Spanned Volumes קיימים המפורמטים NTFS על ידי הוספת שטח פנוי. כלי מנהל הדיסק מפרמט את השטח החדש מבלי להשפיע על קובץ קיים כלשהו ב-Volume המקורי. לא ניתן להרחיב Volumes מפורמטים בשיטות FAT16 או FAT32.

תוכל להרחיב Spanned Volumes על דיסקים דינמיים עד למקסימום של 32 דיסקים. לאחר ש-Volume הורחב למספר דיסקים (ועכשיו הוא נקרא Spanned Volumes), הוא אינו יכול להוות חלק מ-Mirrored Volume או Striped Volume. לאחר הרחבת Spanned Volume, לא ניתן למחוק שום חלק ממנו ללא מחיקתו המלאה. לא ניתן להרחיב System Volume או Boot Volume.

עבודה עם Striped Volumes

Striped Volumes מספקים את הביצועים הטובים ביותר מכל אסטרטגיות ניהול הדיסקים במערכת Windows 2000. ב-Striped Volumes, הנתונים נכתבים בצורה שווה על פני כל הדיסקים הפיסיים ביחידות של 64KB. כיון שכל הדיסקים הקשיחים השייכים ל-Striped Volume מבצעים תפקידים זהים לדיסק קשיח בודד, Windows 2000 יכולה להנפיק ולעבד פקודות קלט/פלט על כל הדיסקים הקשיחים בו-זמנית. בצורה זו, Striped Volume יכולים להגדיל את מהירות הקלט/פלט של מערכת ההפעלה.

Striped Volume נוצר כתוצאה ממיזוג שטחים פנויים במספר דיסקים (2 עד 32) ליצירת Logical Volume אחד גדול. עם Striped Volume, Windows 2000 כותבת נתונים לדיסקים רבים, בדומה ל-Spanned Volumes. אולם, ב-Striped Volumes, מערכת ההפעלה כותבת קבצים על פני כל הדיסקים, כך שהנתונים נוספים לכל הדיסקים בקצב זהה. כמו Spanned Volumes, Striped Volumes אינם מספקים Fault tolerance (סיבולת תקלות). אם דיסק אחד ב-Striped Volume נכשל, המידע כולו ב-Volume הולך לאיבוד.

נדרשים לפחות שני דיסקים דינמיים ליצירת Striped Volume, וניתן ליצור את Striped Volume על מקסימום 32 דיסקים. אולם, לא ניתן להרחיב או לבצע Mirroring על Striped Volume. אפשר להשתמש בתוסף התוכנה Disk Management ליצירת Striped Volume. על הדיסק הדינמי בו תרצה ליצור את ה-Striped Volume, לחץ לחיצה ימנית בשטח הבלתי מוקצה, ואז לחץ Create Volume. אשף Create Volume יופעל וידריך אותך בהליך היצירה של Striped Volume.

התקנת דיסקים

בעת התקנת דיסקים חדשים במחשב המפעיל Windows 2000, הם נוספים כאחסון בסיסי.

התקנת דיסקים חדשים

להתקנת דיסק חדש, התקן או צרף דיסק (או דיסקים) חדש ולחץ על Rescan Disks (סרוק דיסקים שנית) בתפריט תוסף התוכנה Disk Management. יש להשתמש ב-Rescan Disks בכל פעם שתתקין או תסיר דיסקים מהמחשב. לא נדרש לאתחל את המחשב שנית בעת התקנת דיסק חדש במחשב. אולם, ייתכן שתצטרך בכל זאת לאתחל את המחשב מחדש אם Disk Management אינו מזהה את הדיסק החדש לאחר הפעלת Rescan Disks.

התקנת דיסק שהסרת ממחשב אחר

הליך הסרת דיסק ממחשב אחד והתקנתו באחר שונה מהתקנת דיסק חדש. לאחר הסרת הדיסק מהמחשב המקורי והתקנתו במחשב החדש, השתמש ב-Disk Management להתקנת הדיסק. כדי לעשות כן, לחץ לחיצה ימנית על הדיסק החדש שהוספת ולחץ Import Foreign Disk (יבא דיסק זר). האשף שיופיע יספק הוראות התקנה על המסך.

התקנת מספר דיסקים שהוסרו ממחשב אחר

הליך הסרת מספר דיסקים ממחשב אחד והתקנתם במחשב אחר דומה בעיקרו להליך התקנת דיסק בודד שהוסר ממחשב אחר. להתקנת מספר דיסקים מירושה, עליך להסירם מהמחשב המקורי ולהתקינם במחשב החדש. עתה השתמש ב-Disk Management לציון הדיסקים שנדרש להתקין מתוך הקבוצה.

בעת העברת דיסק דינמי ממחשב אחר המפעיל Windows 2000 למחשב שלך, תוכל להשתמש בכל ה-Volumes הקיימים על דיסק זה. אולם, אם Volume על דיסק זר מורחב למספר דיסקים, ואינך מעביר את כל הדיסקים של Volume זה, Disk Management לא יציג את קטע ה-Volume ששוכן על הדיסק הזר.

שינוי סוג אחסון

תוכל לשדרג דיסק מאחסון בסיסי לאחסון דינמי בכל עת, ללא אובדן נתונים. בעת שדרוג דיסק בסיסי לדיסק דינמי, כל המחיצות הקיימות על הדיסק הבסיסי נהפכות ל-Simple Volumes. כל Mirrored Volume, Striped Volume, או Spanned Volume קיים שנוצרו עם Windows NT 4.0 הופכים ל-Dynamic Mirrored Volume, Dynamic Striped Volume או Dynamic Spanned Volume, בהתאמה. Striped Volume של Windows NT 4.0 עם בדיקת זוגיות, מוסב ל-RAID-5 Volume. כדי שהשדרוג יצליח חייב כל דיסק שיש לשדרג להכיל לפחות 1MB שטח דיסק בלתי מוקצה. לפני שדרוג דיסקים, סגור

את כל התוכנות הפועלות על הדיסק. הטבלה להלן מפרטת את התוצאות של הסבת דיסק מאחסון בסיסי לאחסון דינמי.

Basic Disk Organization	**Dynamic Disk Organization**
System Partition	Simple Volume (cannot be extended)
Boot Partition	Simple Volume (cannot be extended)
Primary Partition	Simple Volume
Extended Partition	Simple Volume for each logical drive and any remaining unallocated space
Logical Drive	Simple Volume
Volume Set	Spanned Volume
Striped Set	Striped Volume
Mirror set	Mirrored Volume
Striped set with parity	RAID-5 Volume

הערה יש לגבות תמיד את נתוני הדיסק לפני הסבת סוג האחסון.

שדרוג דיסקים בסיסיים לדיסקים דינמיים

לשדרוג דיסק בסיסי לדיסק דינמי, לחץ לחיצה ימנית על הדיסק הבסיסי שברצונך לשדרג ולחץ Upgrade To Dynamic Disk (שדרג לדיסק דינמי). יופיע אשף שיספק הוראות על המסך. הליך השדרוג דורש כיבוי והפעלה מחדש של המחשב.

לאחר שדרוג דיסק בסיסי לדיסק דינמי, תוכל ליצור Volumes עם יכולות מוגברות על הדיסק, אך הדיסק לא יכול להכיל מחיצות ראשיות או מורחבות. רק Windows 2000 יכולה לגשת לדיסקים דינמיים.

החזרת דיסק דינמי לדיסק בסיסי

לפני שתוכל להחזיר דיסק דינמי לדיסק בסיסי, יש להסיר את כל ה-Volumes מהדיסק הדינמי, כך שהדיסק כולו יהווה שטח בלתי מוקצה. לשינוי דיסק דינמי חזרה לדיסק בסיסי, לחץ לחיצה ימנית על הדיסק הדינמי (כל השטח הבלתי מוקצה) שברצונך להחזיר לדיסק בסיסי, ולחץ Revert To Basic Disk (חזור לדיסק בסיסי).

אזהרה הסבת דיסק דינמי לדיסק בסיסי תגרום לאובדן כל הנתונים.

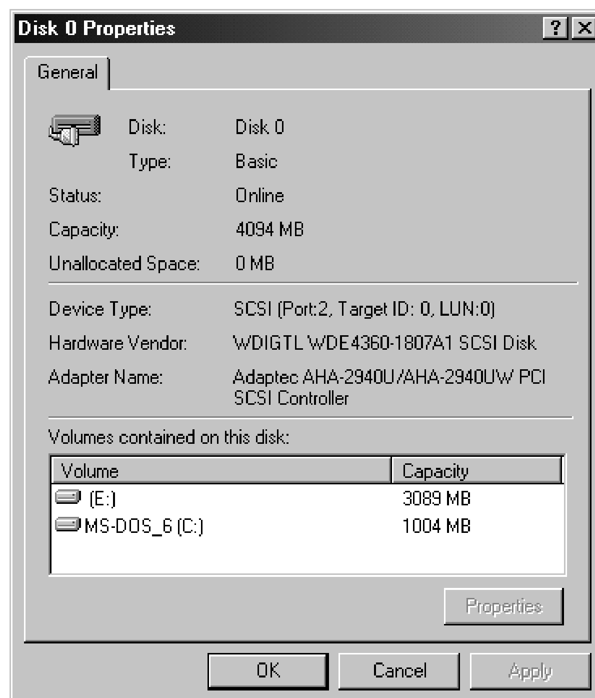
צפייה ועדכון נתונים

תיבת הדו-שיח Properties (תכונות) עבור דיסק או Volume נבחר מספקת תצוגה תמציתית של כל התכונות הנדרשות.

תכונות דיסק

לצפייה בתכונות הדיסק בתוסף התוכנה Disk Management, לחץ לחיצה ימנית על שם הדיסק בחלון התצוגה הגרפית (אל תלחץ על אחד מה-Volumes שלו) ולחץ Properties.

תרשים 4.5 מתאר את מסך תכונות הדיסק.



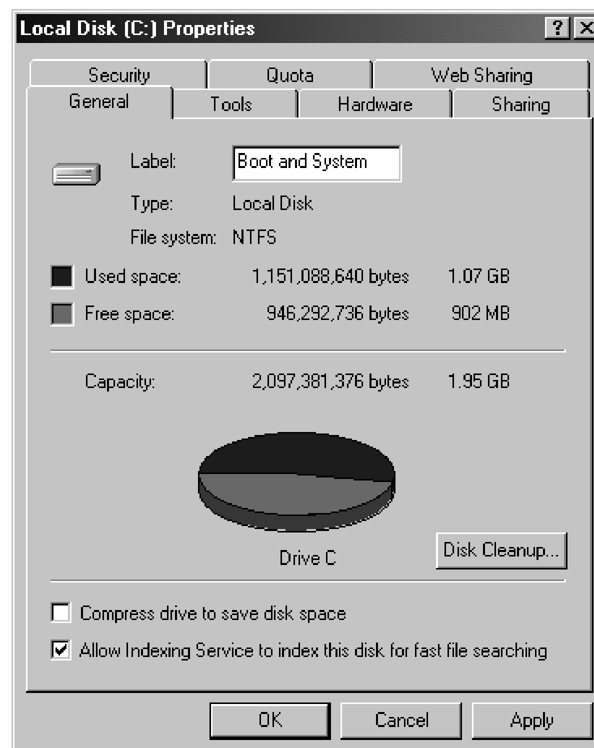
תרשים 4.5 תכונות Disk0 המופיעות בתוסף התוכנה Disk Management.

הטבלה להלן מתארת את המידע המפורט בתיבת הדו-שיח Properties של הדיסק.

סיווג	תיאור
Disk	מספר הדיסק במערכת. לדוגמה, Disk0 , Disk1, Disk2 , וכו׳
Type	סוג האחסון (בסיסי, דינמי או נייד)
Status	מקוון, לא מקוון, זר, או בלתי ידוע
Capacity	סך כל קיבולת הדיסק
Unallocated Space	כמות השטח שלא בשימוש הזמין על הדיסק. שטח פנוי במחיצות דיסק בסיסי או ב-Volumes של דיסק דינמי אינו מופיע כאן.
Device Type	IDE, SCSI, EIDE. כמו כן מציג גם את ערוץ IDE (ראשי או משני) עליו יושב דיסק IDE, ID (זיהוי) יעד, ומספר LUN לזיהוי דיסקים מסוג SCSI.
Hardware Vendor	יצרן הדיסק וסוג הדיסק
Adapter Name	סוג הבקר אליו מחובר הדיסק
Volumes Contained On This disk	ה-Volumes הקיימים על דיסק זה וגודלם הכולל

Volume Properties

לצפייה בתכונות ה-Volume ב-Disk Management, לחץ לחיצה ימנית על Volume בחלון התצוגה הגרפית או בחלון רשימת ה-Volumes ולחץ Properties. תרשים 4.6 מראה את תיבת הדו-שיח עבור ה-Volume המקומי.



תרשים 4.6 תיבת הדו-שיח עבור ה-Volume המקומי.

הטבלה הבאה מתארת את הכרטיסיות בתיבת הדו-שיח של Properties של ה-Volume.

כרטיסיה	תיאור
General	מפרט את תווית ה-Volume, סוג, מערכת קבצים, ושטח פנוי ושטח בשימוש. לחץ Disk Cleanup (ניקוי דיסק) למחיקת קבצים מיותרים. NTFS Volumes הן בעלות שתי אפשרויות: (1) Compress Drive To Save Disk Space (דחוס כונן לחסכון בשטח דיסק), ו- (2) Allow Indexing Service To Index This Drive For Fast File Searching (אפשר לשירות אינדקס ליצור אינדקס עבור כונן זה לחיפוש קבצים מהיר).
Tools	מספק נקודה מרכזית אחת ממנה ניתן לבצע איתור שגיאות ב-Volume, גיבוי, ומטלות Defragmentation (איחוי).
Web Sharing	משמש לשיתוף בקבצים מוגדרים באמצעות IIS (**I**nternet **I**nformation **S**ervices). כרטיסיה זו תופיע רק אם IIS הותקן על Windows 2000 Server או אם הותקן Personal Web Server במערכת Windows 2000 Professional.

כרטיסיה	תיאור
Sharing	משמש לשיתוף פרמטרים והרשאות של Volumes ברשת.
Hardware	משמש לבדיקת תכונות הדיסקים הפיסיים המותקנים במערכת ואיתור תקלות בהם.
Security	משמש להגדרת הרשאות גישה של NTFS. כרטיסיה זו זמינה רק עבור NTFS Volumes בגרסאות 4.0 ו- 5.0 (Windows 2000 משתמשת ב-NTFS גירסה 5.0).
Quota	משמש להגדרת מכסות משתמשים עבור NTFS 5.0 Volumes.

רענון וסריקה חוזרת (Refresh and Rescan)

בעת עבודה עם Disk Management ייתכן שיתעורר צורך לעדכן את המידע בתצוגה. שתי הפקודות לעדכון התצוגה הן Refresh (רענון) ו-Rescan (סריקה חוזרת).

Refresh – מעדכנת אותיות כוננים, מערכות קבצים, Volumes ומידע על מדיה ניידת, וקובעת אם Volumes בלתי ניתנים לקריאה הם עתה ניתנים לקריאה. לעדכון אות הכונן, מערכת הקבצים ונתוני ה-Volume, לחץ Action ואז לחץ Refresh.

Rescan Disks – מעדכנת נתוני חומרה. כאשר Disk Management סורק דיסקים שנית, הוא סורק את כל הדיסקים המחוברים לאיתור שינויי תצורה בדיסק. כמו כן הוא גם מעדכן מידע אודות מדיה ניידת, כונני תקליטורים, basic volumes, מערכות קבצים ואותיות כוננים. סריקה חוזרת של דיסקים עלולה לארוך מספר דקות, בהתאם למספר התקני החומרה המותקנים. לעדכון נתוני הדיסק, לחץ Action ואז לחץ Rescan Disks.

הערה אם אתה מפעיל את תוסף התוכנה Computer Management, בחר בצומת Disk Management או כל אובייקט בצומת זו כדי להתחיל את פעולת הרענון או הסריקה החוזרת.

ניהול דיסקים במחשבים מרוחקים

כחבר בקבוצת Administrator, תוכל לנהל דיסקים על מחשב המפעיל Windows 2000 שהוא עמית באותה קבוצת עבודה, domain או Trusted domain (אמון/סמיכות), מכל מחשב אחר המפעיל Windows 2000 ברשת.

לניהול מחשב אחד ממחשב אחר - ניהול מרחוק - צור MMC (**M**icrosoft **M**anagement **C**onsole), ומקד אותה על המחשב המרוחק. MMC תידון ביתר הרחבה בפרק 5.

תרגיל 1: הגדרת דיסק פשוט והסבתו לדיסק דינמי

תרגיל זה דורש התקנת מערכת Windows 2000 Server כמפורט בפרק 2 וקיום שטח דיסק בלתי מוקצה על Server01 כמפורט בהקדמה.

הליך 1: התקנת FTP

על Server01, תתקין שרת FTP לצורך השלמת השלבים שבהליך 2. ראה פרק 14, שיעור 2: "ניהול סביבת אינטרנט", לפרטים אודות שירות שרת זה.

1. הכנס את תקליטור Windows 2000 Server לכונן התקליטורים.
2. לחץ על לחצן Start, הצבע על Settings, ולחץ על Control Panel. לוח הבקרה יופיע.
3. לחץ לחיצה כפולה על היישומון Add/Remove Programs. יופיע חלון Add/Remove Programs.
4. בחלונית השמאלית, לחץ Add/Remove Windows Components. יופיע חלון אשף Windows Components.
5. בתיבה Components, לחץ פעם אחת על (IIS) Internet Information Services, ולחץ על לחצן Details. תופיע תיבת הדו-שיח של Internet Information Services (IIS).
6. בתיבת הדו-שיח Subcomponents of Internet Information Services (IIS), סמן את תיבת סימון File Transfer Protocol (FTP) Server.
7. לחץ OK. אשף הרכיבים של Windows יופיע.
8. לחץ Next. יופיע מסך Configuring Components (מגדיר רכיבים) בעוד שינוי התצורה שבקשת מתבצעים. לאחר מספר דקות יופיע מסך Completing the Windows Components.
9. לחץ Finish. יופיע חלון Add/Remove Programs.
10. לחץ Close. לוח הבקרה יופיע.
11. סגור את לוח הבקרה.

הליך 2: שימוש בתוסף התוכנה Disk Management

על Server01, תיצור מחיצות ראשיות רבות ומחיצה מורחבת בחלק הבלתי מוקצה של Disk0. להתחלת הליך זה, התחבר ל-Server01 בשם משתמש Administrator עם הסיסמה password.

1. לחץ על לחצן Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ Computer Management. תוסף התוכנה Computer Management יופיע.

2. מהחלונית השמאלית, הרחב את צומת Storage (אחסון) ובחר Disk Management.

בחלונית הימנית יופיעו חלון Volume List (בחלק העליון) וחלון התצוגה הגרפית (בחלק התחתון). שים לב ש-Disk0 מורכב ממחיצה ראשית :C ושאר שטח הדיסק אינו מוקצה.

3. לחץ על השטח הבלתי מוקצה בתצוגה הגרפית.

4. בתפריט Action, לחץ All Tasks ובחר Create Partition.

יופיע אשף Create Partition.

5. קרא את המידע המופיע ב- Welcome To The Create Partition Wizard, ולחץ Next.

6. ממסך Select Partition Type, ודא שלחצן האפשרויות של המחיצה הראשית מסומן, ולחץ Next.

7. ממסך Specify Partition Size, שנה את ערך Amount Of Disk Space To Use ל- 50, ולחץ Next.

8. ממסך Assign Drive Letter Or Path, שנה את אות השיוך :Assign A ל- :H, ולחץ Next.

9. ממסך Format Partition, ודא שנבחר לחצן אפשרויות Format This Partition With The Following Settings, לחץ על תיבת סימון Perform A Quick Format, ולחץ Next.

10. עיין במידע המופיע על מסך אשף Completing The Create Partition, ולחץ Finish.

לאחר שמערכת Windows 2000 Server השלימה את הבקשה של יצירת מחיצה, תופיע מחיצה :H בחלון התצוגה הגרפית.

11. אם מופיעה תיבת הודעות System Change המנחה לכבות ולחזור ולהפעיל את המחשב, לחץ Yes לעשות כן. לאחר שההפעלה החוזרת הושלמה, התחבר למחשב שנית כמנהל עם הסיסמה password.

12. חזור ובצע את השלבים הקודמים בהליך זה, וצור את תצורות הדיסק הבאות בשטח הבלתי מוקצה של Disk0. השתמש בטבלה להלן לשנות ערכים בהליך הקודם:

סוג מחיצה	גודל (MB)	כונן דיסקים	פורמט
ראשי	100	1	FAT32
מורחב	שטח בלתי מוקצה נותר	לא ידוע	לא ידוע

13. עיין בהגדרות עבור כונן :H ו-:I בחלון Volume View. שים לב ששטח הדיסק הפנוי המופיע בתצוגה הגרפית אינו כולל אותיות כוננים. שטח זה הוא השטח המורחב שבו תקצה כוננים לוגיים.

14. בחלון התצוגה הגרפית, לחץ על תיבת Free Space במחיצה המורחבת.

15. בתפריט Action, בחר All Tasks ומשם בחר Create Logical Drive.

אשף יצירת המחיצה יופיע.

16. קרא את המידע המופיע ב- Welcome To The Create Partition Wizard, ולחץ Next.

17. ממסך Select Partition Type, ודא שלחצן האפשרויות Logical Drive מסומן, ולחץ Next.

18. במסך Specify Partition Size, שנה את ערך Amount Of Disk Space To Use ל- 150, ולחץ Next.

19. במסך Assign Drive Letter Or Path Screen, בחר בלחצן אפשרויות Mount This Volume At An Empty Folder That Supports Drive Paths, ולחץ Browse.

תופיע תיבת דו-שיח Browse For Drive Path.

20. הרחב את כונן \:C ולאחריו הרחב את Inetpub.

21. לחץ בתת התיקיה ftproot, ולחץ OK.

לחצן האפשרויות Mount This Volume At An Empty Folder That Supports Drive Paths יורה על הנתיב C:\Inetpub\ftproot.

22. לחץ Next.

23. ממסך Format Partition, בצע פרמוט מהיר ליצירת מחיצה NTFS, שנה את תווית ה-Volume ל- FTPVol, ואפשר דחיסת קבצים ותיקיות.

24. לחץ Next.

25. עיין במידע המופיע על מסך אשף Completing The Create Partition, ולחץ Finish.

שים לב שכיון שהליך זה לא דרש הגדרת שמות Volumes, מחיצות :I ו- :J מציגים שמות Volumes של (:NEW VOLUME (H ו- (:NEW VOLUME (I בהתאמה.

26. לשינוי שמות ה-Volumes, לחץ על (:NEW VOLUME (H ב- Volume View או בחלון התצוגה הגרפית.

27. מתפריט Action, בחר All Tasks, ומשם Properties.

תופיע תיבת דו-שיח New Volume (H:) Properties.

28. בתיבת הטקסט Label מחק New Volume ולחץ OK.

29. חזור ובצע את שלושת השלבים האחרונים עבור (:NEW VOLUME (I.

תצורת הדיסק עבור Disk0 צריכה עתה להיות כדלקמן :

כונן/נתיב	פורמט	סוג	מטרה
C:	NTFS	ראשי	מערכת (כולל גם את מחיצת האתחול, אף כי זה אינו מופיע בתוסף התוכנה Disk Management)
H:	NTFS	ראשי	לא בשימוש
I:	FAT32	ראשי	לא בשימוש
C:InetPub\ftproot	NTFS	מורחב	קבצים הנשמרים ל-C:InetPub\ftproot מנותבים למחיצת דיסק זו.
לא ידוע	לא ידוע	מורחב	שטח פנוי. (גודל השטח הפנוי ישתנה בהתאם לגודל Disk0).

30. כדי לבדוק ש-FTPVol היא מחיצה זמינה ל-C:InetPub\ftproot, פתח את סייר Windows.

31. הרחב את My Computer מהחלונית השמאלית והרחב את C:InetPub.

שים לב ש-ftproot מופיע כסמל כונן. כל הקבצים המאוחסנים ב-C:InetPub\ftproot מנותבים ל-FTPVol במחיצה המורחבת.

32. סגור את סייר Windows ואת תוסף התוכנה Computer Management.

סיכום שיעור

לפני שתוכל לאחסן נתונים על דיסק קשיח חדש, יש לאתחל את הדיסק על ידי הגדרת סוג אחסון, מחיצות ופורמט. Windows 2000 תומכת באחסון בסיסי ואחסון דינמי. דיסק בסיסי יכול להכיל מחיצות ראשיות, מחיצות מורחבות וכוננים לוגיים במחיצה המורחבת. עבור Windows 2000 אחסון בסיסי הוא ברירת המחדל, כך שכל הדיסקים הם דיסקים בסיסיים עד שתסב אותם לדיסקים דינמיים. אחסון דינמי יוצר מחיצה בודדת הכוללת את הדיסק כולו. מחלקים דיסקים דינמיים ל-Volumes, שיכולים להכיל קטע או קטעים של דיסק פיסי אחד או יותר. תוסף התוכנה Disk Management מספק נקודה מרכזית לכל המידע אודות הדיסק ועבור מטלות הניהול כגון יצירה ומחיקת Partitions ו-Volumes. עם ההרשאות המתאימות, תוכל לנהל דיסקים מקומיים או דיסקים על מחשבים מרוחקים. בנוסף לניטור נתוני הדיסק, מטלות ניהול דיסקים נוספות שאולי תצטרך לבצע כוללות הוספה והסרה של דיסקים ושינוי סוג אחסון הדיסק.

שיעור 2:
FAT - File Allocation Table

Windows 2000 תומכת בשתי גרסאות של מערכת קבצים **F**ile **A**llocation **T**able - FAT: FAT16 ו-FAT32. שיעור זה מהווה סקירה של שתי מערכות קבצים אלו, ושימושן בתוך מערכת ההפעלה Windows 2000.

לאחר שיעור זה, תוכל

- לתאר את מערכת הקבצים FAT16 של Windows 2000.
- לתאר את מערכת הקבצים FAT32 של Windows 2000.

זמן לימוד משוער: 25 דקות

מבוא למערכת קבצים FAT

מערכת קבצים FAT תוכננה כאשר הדיסקים היו קטנים יותר ומבנה התיקיות היה פשוט. להגנת מערכת הקבצים, מאוחסנים ב-Volume שני העתקים של FAT (טבלת הקצאת קבצים). במקרה שהעתק אחד של הטבלה נהרס, נעשה שימוש בהעתק השני. טבלת ההקצאה של הקבצים מאוחסנת ב- Specified Byte Offset (היסט סיביות מוגדר), כך שהקבצים הנדרשים לאתחול המערכת ניתנים לאיתור.

FAT16 פועלת ב-Windows 2000 בצורה זהה לאופן פועלתה ב-MS-DOS, Windows 3.x, Windows 95, Windows 98. FAT32 פועלת ב-Windows 2000 בצורה זהה לאופן פעולתה ב-Windows 95 OSR2, ו-Windows 98. ניתן להתקין את Windows 2000 על מחיצה ראשית FAT קיימת או כונן לוגי. בעת הפעלת Windows 2000, ניתן להזיז או להעתיק קבצים בין FAT Volumes ו-NTFS Volumes.

לא ניתן להשתמש ב-Windows 2000 בתוכנות דחיסה או חציצה הדורשות טעינת מנהל התקן דיסק דרך MS-DOS. אי לכך, לא ניתן להשתמש ב-MS-DOS 6.0 DoubleSpace או MS-DOS 6.22 DiskSpace על מחיצה ראשית FAT או כונן לוגי שאליו ברצונך לגשת בעת הפעלת Windows 2000.

מערכת קבצים FAT16

פורמט FAT מאורגן לסקטורים (מקטעים). כל **סקטור** (Sector) יכול לאחסן 512 סיביות של נתונים. זוהי היחידה הקטנה ביותר המשמשת לקריאה או כתיבה מהדיסק ואליו.

אף שסקטור היא היחידה הקטנה ביותר המשמשת להעברת נתונים ממחיצת FAT ואליה, ה**אשכול** (Cluster, ידוע גם כ-Allocation Unit - יחידת הקצאה), הוא היחידה הקטנה ביותר המשמשת את מערכת ההפעלה בעת הקצאת שטח אחסון קבצים במחיצת FAT. גודל האשכול משתנה מכונן לכונן, בהתאם לגודל המחיצה. גודל ברירת המחדל של האשכול (Cluster) נקבע על ידי גודל המחיצה ויכול להיות אף בגודל 64KB.

טבלת ההקצאה של הקבצים מזהה כל אשכול במחיצה כאחד מהבאים:

- לא בשימוש.
- אשכול בשימוש על ידי קובץ.
- אשכול פגום.
- אשכול אחרון בקובץ.

הערה Volumes בגודל של פחות מ- 16MB יפורמטו לרוב ל-FAT של 12 סיביות, אך הגודל המדויק תלוי בגיאומטריית הדיסק. FAT12 היה היישום הראשון של FAT. הוא מיועד למדיה קטנה ביותר. בכך שפחות שטח נצרך עבור כל רישום FAT, השטח הנצרך על ידי ה-FAT קטן יותר. אי לכך, יותר שטח זמין לנתונים בניגוד למבנה קבצים על דיסק. כיום, משתמשים יפגשו FAT12 רק במדיה קטנה מאוד או ישנה. לדוגמה, דיסקטים 3.5 אינץ' הם FAT16 בעוד שדיסקטים 5.25 אינץ' הם FAT12.

תרשים 4.7 מתאר מבנה FAT16 Volumes. תיקיית השורש כוללת רישום עבור כל קובץ ותיקיה ב-Volume. ההבדל היחיד בין תיקיית השורש לתיקיות אחרות הוא שתיקיית השורש היא במיקום מוגדר על הדיסק ויש לה גודל קבוע של 512 רישומי טבלה עבור כל כונן דיסקים. מספר הרישומים על דיסקט תלוי בגודלו של הדיסקט.

Boot sector
on system (active) partition

File Allocation Table (FAT)
primary

File Allocation Table (FAT)
copy for fault tolerance

Root folder
fixed location and length (512 entries long)

Other folders and all files

תרשים 4.7 מבנה FAT16 Volume.

לתיקיות יש רישום של 32 סיביות עבור כל קובץ ותיקיה הכלולים בתיקיה. הטבלה שלהלן היא רשימה של רכיבי הרישום של הקבצים והתיקיות.

רכיב רישום	סיביות
Name (שם)	פורמט 8.3
Attribute (מאפיין)	8
Create time (זמן יצירה)	24
Create date (תאריך יצירה)	16
Last access date (תאריך גישה אחרון)	16
Last modified time (זמן עדכון אחרון)	16
Last modified date (תאריך עדכון אחרון)	16
Starting cluster number in FAT (מספר אשכול ראשון ב-FAT)	16
File size (גודל קובץ)	32

מבנה התיקיות של FAT אינו מאורגן. קבצים מקבלים את המיקום הזמין הראשון ב-Volume. מספר האשכול הראשון הוא הכתובת של האשכול הראשון המשמש את הקובץ. כל אשכול כולל מצביע לאשכול הבא בקובץ או מזהה hex (OxFFFF) שאשכול זה הוא סוף הקובץ.

המידע בתיקיה משמש את כל מערכות ההפעלה התומכות במערכת קבצים FAT. מערכות הפעלה Windows NT יכולות לרשום חותמות זמן נוספות ברישום תיקיית FAT. חתימות זמן אלה מורות מתי הקובץ נוצר או מתי ניגשו אליו לאחרונה; הן

משמשות בעיקר ביישומים של **P**ortable **O**perating **S**ystem **I**nterface Standard (POSIX, תקן ממשק מערכות הפעלה ניידות).

כיון שכל הרישומים בתיקיה זהים בגודלם, ה-Attribute Byte (הבית המאפיין) לכל רישום בתיקיה מתאר איזה סוג רישום זה. לדוגמה, סיבית אחת מצביעה על כך שהרישום הוא עבור תת תיקיה, סיבית אחרת מסמנת את הרישום כתווית Volume. במצב רגיל, רק מערכת ההפעלה שולטת על ההגדרות של סיביות אלה.

הבית המאפיין כולל ארבע סיביות הניתנות לכיבוי והפעלה על ידי המשתמש:

- קובץ ארכיון.
- קובץ מערכת.
- קובץ נסתר.
- קובץ לקריאה בלבד.

מערכת הקבצים FAT16 נכללת ב-Windows 2000 לצורך תמיכה לאחור במוצרי Windows קודמים. בנוסף, FAT16 מאפשרת תאימות רחבה עם מערכות הפעלה אחרות שאינן מתוצרת Microsoft.

כבגרסאות קודמות, גודל המחיצה המירבי של FAT16 במערכת Windows 2000 הוא 4GB. גודל ברירת המחדל של ה**אשכול** (Cluster) נקבע על ידי גודל המחיצה. הטבלה הבאה מציגה את גדלי ברירת המחדל של האשכולות עבור FAT16 Volumes:

גודל המחיצה	סקטורים בכל אשכול	גודל האשכול
0MB-32MB	1	512 בתים (שווה ערך לגודל סקטור המחיצה)
33MB-64MB	2	1024 בתים
65MB-128MB	4	2048 בתים
129MB-256MB	8	4096 בתים
256MB-512MB	16	8192 בתים
512MB-1024MB	32	16KB
1024MB-2048MB	64	32KB
2048MB-4096MB	128	64KB

תוכל להגדיר גודל אשכול אחר אם תשתמש בתוכנית השירות Format עם מתג /a:size משורת הפקודה לפרמוט המחיצה. אולם, הגדרות ברירת המחדל מומלצות לשימוש רגיל.

הערה דיסקים היכולים לתמוך בסקטורים הגדולים יותר מ- 512 בתים יכולים ליצור אשכולות של 128KB ו- 256KB. אולם, ככל שגודל האשכול גדול יותר כך קיים פוטנציאל גדול יותר לבזבוז שטח דיסק. אשכולות גדולים מתאימים במיוחד לקבצים גדולים מאוד, כמו בסיסי נתונים.

מערכת קבצים FAT32

היתרון העיקרי של FAT32 הוא ביכולתה לתמוך במחיצות גדולות יותר מאלו שמערכת קבצים FAT16 יכולה לטפל. FAT16 תומכת במחיצות בגודל של עד 4GB, בעוד ש-FAT32 תומכת במחיצות עד 2047GB. אולם, יישומי FAT32 של Windows 2000 מוגבלים ליצירת Volumes בגודל של עד 32GB, אף ש- FAT32 Volumes קיימות הגדולות מ-32GB יכולות להיות מותקנות. פרט להגבלת פרמוט מחיצות זו, תכונות ופרמוט דיסק של FAT32 זהים עבור Windows 2000 לאלה שהיו ב-OSR2 Windows 95 ו-Windows 98.

לשמירה על תאימות גדולה ככל הניתן עם תוכנות קיימות, רשתות ומנהלי התקנים, FAT32 מיושמת עם שינויים קטנים ככל הניתן למבנה FAT16 הקיים, מבני נתונים פנימיים, **A**pplication **P**rogramming **I**nterfaces (API, ממשקים של יישומי תוכנה) ופקודת Format כפקודה פנימית (ללא צורך בדיסקט חיצוני להפעלתה).

אולם, כיון שעתה נדרשים ארבעה בתים בטבלה לאחסון ערכי אשכולות, מבני נתונים פנימיים ועל-הדיסק ו-API רבים שהוצאו לאור, שונו או הורחבו. במקרים מסוימים API קיימים בוטלו, כדי למנוע נזק לכונני FAT32 על ידי תוכניות שירות מיושנות. אולם, רוב התוכנות לא יושפעו משינויים אלה. כלים ומנהלי התקנים קיימים של FAT אמורים להמשיך ולעבוד על מחיצות FAT32. יש לעדכן כלי דיסק של מערכות הפעלה MS-DOS לתמיכה בהתקני FAT32.

מבנה מחיצות FAT32

היתרון העיקרי של FAT32 על פני FAT16 הוא תמיכה במחיצות גדולות יותר. FAT32 מתגבר על מגבלת גודל מחיצה של 4GB, על ידי הגדלת קיבולת המחיצה. אם אתה מפרמט מחיצה עם FAT16, עליך להגדיר אשכול של 32KB לפחות כדי לתמוך במחיצה של 4GB או יותר.

גודל הקובץ המירבי לכונן של FAT32 הוא 4GB פחות שני בתים. FAT32 מקצה ארבעה בתים בטבלת הקצאת הקבצים (File Allocation Table) עבור כל אשכול. לעומתו, מערכת קבצים FAT16 מקצה רק שני בתים עבור כל אשכול.

מחיצת FAT32 חייבת להכיל לפחות 65,527 אשכולות, וגודל המחיצה אינו ניתן להגדלה. תרשים 4.8 מתאר את מבנה מחיצת FAT32.

Boot sector points to
the first cluster of the root folder.

Root folder can be located anywhere on disk,
boot sector points to it. Limit to 65,535 entries.

File Allocation Table (FAT)
primary

File Allocation Table (FAT)
secondary–mirroring of primary can be disabled for performance.

Other folders and all files
varies

תרשים 4.8 מבנה FAT32 Volume.

מערכות קבצים FAT32 ו-FAT16 לא מתמודדות בצורה טובה עם נפחים גדולים. ככל שה-Volume גדול יותר, טבלת ההקצאה של הקבצים גדולה אף היא. אחד החסרונות של טבלת הקצאת הקבצים גדולה הוא שהזמן שלוקח למערכת ההפעלה לחשב את כמות השטח הפנוי הזמין ב-Volume האתחול, גדל בצורה דרמטית בעת האתחול.

טבלת הקצאת הקבצים היא רשימה דחוסה של רישומים בני 32 סיביות הממופים אחד לאחד עם אשכולות הנתונים. מבנה התיקיות של FAT32 משמש באופן דומה לצורה בה Windows 95 מיישמת שמות קבצים ארוכים. ההבדל היחיד היא תוספת של שדה High Word לאשכול ברישומי הספריות הניגשים למספרי האשכולות.

מגבלות מערכת הקבצים

הגודל המירבי של FAT32 Volume מוגבל על ידי המספר המירבי של רישומי FAT, מספר הסקטורים בכל אשכול, ומונה הסקטורים בן 32 סיביות שברישומי המחיצה (ההנחה היא שהסקטורים הם בני 512 בתים כל אחד).

הטבלה הבאה ממפה את גודל המחיצה המירבי האפשרי עבור כל אשכול:

גודל האשכול	גודל Volume מירבי
512 בתים	127.9GB
1KB	255.9GB
2KB	511.9GB
4KB	1023.9GB (או 1TB)
8KB	2047GB (2TB)
16KB	2047GB (2TB)
32KB	2047GB (2TB)

קח בחשבון ש-Windows 2000 מגבילה את גודל המחיצה ל- 32GB אך תטען מחיצות FAT32 גדולות יותר שנוצרו במערכות הפעלה אחרות, כגון Windows 98.

סיכום שיעור

מערכת קבצים FAT תוכננה עבור דיסקים קטנים ומבנה תיקיות פשוט. Windows 2000 תומכת בשתי גרסאות של FAT: FAT16 ו- FAT32. מחיצה המפורמטת עם FAT16 מחולקת לסקטורים בני 512 בתים, והקבצים נכתבים לדיסק כאשכולות (Clusters), הידועים גם כיחידות הקצאה. גודל ברירת המחדל של האשכול נקבע על ידי גודל המחיצה והוא יכול להיות קטן אף כ- 4KB, או שמונה סקטורים, או גדול עד 64KB, או 128 סקטורים. היתרון העיקרי של FAT32 הוא יכולתו לתמוך במחיצות גדולות יותר מאשר FAT16. FAT16 תומך במחיצות בגודל של עד 4GB, בעוד ש-FAT32 יכול לתמוך במחיצות עד לגודל של 2047GB. Windows 2000 תפרמט מחיצות עם FAT32 רק עד גודל של 32GB, אך היא יכולה לטעון מחיצות FAT32 שגודלן 2047GB. FAT32 יושם עם מעט שינויים ככל שניתן למבנה FAT16 קיים, מבני נתונים פנימיים, API - **A**pplication **P**rogramming **I**nterfaces ופרמוט על הדיסק.

שיעור 3:
NTFS - NT File System

Windows 2000 מגיעה עם גירסה חדשה של NTFS. גירסה חדשה זו (NTFS גירסה 5.0) מספקת ביצועים, אמינות ותאימות שאינה מצויה ב-FAT. מבנה הנתונים של NTFS מאפשר ניצול תכונות חדשות ב-Windows 2000, כגון Active Directory Services, תוכנות ניהול ותכונות אחסון המבוססות על נקודות Reparse (חלוקה). NTFS כוללת תכונות אבטחה הנדרשות עבור שרתי קבצים ומחשבי איכות אישיים בסביבת חברות ענק, והיא גם כוללת שליטה על נגישות למידע וזכויות בעלות החשובים לשלמות הנתונים.

לאחר שיעור זה, תוכל

- לתאר את מערכת הקבצים NTFS של Windows 2000.

זמן לימוד משוער: 45 דקות

מבוא ל-NTFS

Microsoft ממליצה שתפרמט את כל המחיצות של Windows 2000 עם NTFS, פרט לתצורות אתחול כפול, בהן נדרשות מערכות הפעלה שאינן Windows 2000 או Windows NT. פרמוט מחיצות Windows 2000 עם NTFS במקום FAT, מאפשר ניצול תכונות הקיימות רק ב-NTFS, כולל התאוששות ודחיסה. ההתאוששות המובנית לתוך NTFS, היא כזו שלעיתים רחוקות יהיה צורך להפעיל תוכנת תיקון דיסקים על NTFS Volume. NTFS מבטיחה את עקביות ה-Volume באמצעות ניהול יומן פעילות תקני (Standard Transaction Logging) וטכניקות התאוששות. בנוסף, Windows 2000 תומכת בדחיסה של קובץ או תיקיה בודדת במחיצת NTFS. קבצים שנדחסו במחיצת NTFS יכולים להיקרא ולהיכתב על ידי כל יישום הפועל תחת Windows 2000, מבלי שיהיה צורך לפרוס אותם קודם באמצעות תוכנית פריסה.

NTFS תומכת בכל תכונות מערכת ההפעלה של Windows 2000. היא מספקת מהירות גישה גבוהה יותר מאשר FAT וממזערת את מספר הגישות לדיסק הנדרשות לאיתור קובץ. בנוסף, NTFS מאפשרת הגדרת הרשאות מקומיות עבור קבצים ותיקיות המגדירות לאיזה קבוצות ומשתמשים הן תהינה נגישות. זה כולל הגדרה של רמת הגישה המותרת. הרשאות NTFS עבור קבצים ותיקיות ישימות גם עבור משתמשים העובדים במחשב בו מאוחסן הקובץ, וגם למשתמשים הניגשים לקובץ דרך הרשת, כאשר הקובץ הוא בתיקיה משותפת. עם NTFS ניתן גם להגדיר זכויות שיתוף בתיקיות משותפות בשילוב עם הרשאות קבצים ותיקיות. FAT תומכת רק בזכויות שיתוף.

טיפ אל תגדיר זכויות שיתוף בתיקיות במחיצות NTFS. במקום זאת, הגדר הרשאות NTFS מקומיות.

תכונות Windows 2000

כל התכונות החדשות והשיפורים ב-Windows 2000 נתמכים על ידי מערכת קבצים NTFS. חלק זה סוקר רבות מהתכונות ואת התייחסותן ל-NTFS.

נקודות חלוקה (Reparse Points)

כדי שמערכת ההפעלה תוכל להתמודד ביתר קלות עם מחיצות NTFS גדולות מאוד, קיימות נקודות המחלקות את המחיצה להרבה תת-מחיצות ובכך היא משפרת את זמני הגישה לקריאה/כתיבה במחיצה. פעילות זו שקופה למשתמש ובאחריות מערכת ההפעלה.

נקודות Reparse (חלוקה) הן אובייקטים חדשים של מערכת קבצים NTFS, המשמשות ב-Windows 2000. **Reparse Point** (נקודת חלוקה) היא קובץ או תיקיה בה מאוחסנים נתונים המבוקרים על ידי המשתמש ב-Reparse Attribute, המנוהל על ידי המערכת. **Reparse Attribute** (מאפיין נקודת חלוקה) משמש מסנני מערכת קבצים לשיפור ההתנהגות הרגילה של קבצים או תיקיות הקיימות בתשתית מערכת הקבצים. כך, קובץ או תיקיה המכילים נקודות Reparse מקבלים תכונות התנהגות נוספות, שאינן קיימות בתשתית מערכת הקבצים.

נקודות Reparse מאפשרות למסנני מערכות קבצים (File System Filters) מרובדות להוסיף תכונות התנהגות מבוקרות-משתמש לקובץ או תיקיה. המנגנון היסודי של נקודת Reparse משנה ומתאים את הליך חלוקת השמות האופייני לקבצים, ומאלץ את התחלתו מחדש עם שם חדש, בעל קונטקסט מבוקר-משתמש. אם נקודת Reparse כוללת נתוני חלוקה פרטיים, הנתונים הללו מוחזרים בחוצץ (Buffer) מתאים והופכים זמינים לכל מסנני קבצי המערכת במערכת.

תגי Reparse משמשים להבחנה בין נקודות Reparse שונות. כאשר נתקלים באובייקט מערכת קבצים בו מאפיין נקודת חלוקה (Reparse Point Attribute), בעת קביעת שמות נתיב, הוא מועבר בחזרה במעלה שכבות מנהלי ההתקנים של מערכת הקבצים עד לחלוקת קלט/פלט (I/O reparse). מסנן מערכת הקבצים מטפל בחלוקת הקלט/פלט, הכולל זיהוי תג Reparse. מנהלי התקנים של מערכות קבצים מבצעים תפקודי קלט/פלט ייחודיים. מנהלי התקנים אלה משתמשים בתג Reparse ובמזהה גלובלי ייחודי (**G**lobal **U**nique **Id**entifier - GUID) לזיהוי קריאות קלט/פלט שהם אחראים להן. על אף שתג החלוקה עצמו הוא ייחודי, GUID מספק זיהוי נוסף.

כאשר משתמש ניגש לתיקיה (Directory Junction), שלה מאפיין נקודת Reparse, מתרחשות מספר פעולות :

1. משתמש פותח Windows 2000 Explorer ולוחץ לחיצה כפולה על NTFS volume.
2. הקריאה עוברת ממצב משתמש למצב ליבה (Kernel), בנקודה בה הוא מגיע לאובייקט מערכת הקבצים ונתקל במאפיין נקודת Reparse התואם.

3. כל File system filter driver בר התקנה של מחסנית הקלט/פלט של Windows 2000 בוחן את התג המשויך לנקודת Reparse. אם יש התאמה, File system filter driver מקבל את הקריאה. מסנני מערכת הקבצים בודקים קריאות נכנסות ויוצאות גם יחד.

4. NTFS directory junction filer drive מקבל את הקריאה ומבצע את התפקודיות המשופרת המשויכת לנקודות Reparse. במקרה של צומת ספריות, מנהל ההתקן טוען טווח שמות נוסף.

5. File system driver מחזיר את הקריאה ליישום הקורא. מנהל התקן מערכת הקבצים טוען טווח שמות נוסף ומחזיר ידית (Handle) לפעולת הקריאה.

הערה אם directory junction נמחק, נקודת Reparse לא תהיה נוכחת. אי לכך, הקריאה לפתיחת תיקיה לא תתקבל על ידי אחד ממנהלי ההתקנים של מערכת הקבצים במחסנית הקלט/פלט, והתוצאה תהיה התנהגות רגילה (ללא חלוקה).

Windows 2000 מאפשרת שינוי הסדר היחסי של מחסניות קבצי המערכת. תוך שימוש במידע השמור ברישום (Registry), ניתן להתקין מסנן מעל או מתחת מסנן אחר. NTFS מותקנת תמיד מתחת למסנני מערכת הקבצים הדורשים ש-NTFS תשמש כשירות, ומעל מנהלי ההתקנים המשמשים את NTFS.

תת מערכת הקלט/פלט של Windows 2000, בונה את מבני הנתונים המתאימים לשרת בקשות ומנהלת את קריאת השכבות לפי תור. לאחר שפעולה עובדה על ידי המחסנית, תת המערכת של הקלט/פלט של Windows 2000 בוחנת את תוצאות הפעולה, ומנפיקה הוראות עבודה נוספות, או מכשילה הוראות עבודה הפועלות כרגיל (שאינן מחולקות).

שני שיפורים שנקודות Reparse מספקות למערכות קבצים הן :

- **ניהול אחסון היררכי** – קבצים שאינם בשימוש מועברים באופן אוטומטי לארכיב זול יותר כמו קלטות או כונן נייד. כאשר משתמש מנסה לגשת לקובץ שהועבר לארכיב, נקודת Reparse מסייעת למערכת ההפעלה לאתר את הקובץ במדיה החליפית. עבור המשתמש, הקובץ נראה זמין כאילו אינו בארכיב.
- **נקודת טעינה של Volume** – מאפשרת למשתמש לעיין במספר Volumes בדיסק כאילו הן כונן בודד.

(Native Structured Storage) NSS

NSS היא תכונה חדשה של Windows 2000. NSS מאפשר אחסון פיסי של מסמכי ActiveX בפורמט Multistream זהה המשמש את ActiveX לעיבוד לוגי של אחסון מובנה. מסנן מערכת קבצי NSS גורם לכך שקובץ על הדיסק ייראה כקובץ אחסון בעל מבנה OLE. התוצאה היא יעילות מוגברת של אחסון פיסי של מסמכי ActiveX מורכבים. כל נתון משובץ של האובייקט שוכן עתה ב-Stream שלו בתוך הקובץ. משמעות עדכון אובייקט היא ש-Stream חדש נוצר עבור האובייקט החדש ושה-Stream המקורי עבור האובייקט נהרס, וגורם למערכת הקבצים לחזור ולקבל בחזרה את שטח הדיסק. מסנן

מערכת קבצים NSS גורם שכל זה יהיה שקוף ליישום. מסנן NSS מאפשר גם שקובץ NSS יועתק לדיסקט, תוך הסבת הקובץ למבנה הקובץ הישן ובחזרה.

Windows 2000 דורשת הנחת נקודת Reparse בכל קובץ המשתמש ב-NSS. נקודת Reparse בקובץ מבצעת את הפעולות הבאות:

- מציינת שלקובץ יש מספר Streams (זרמים).
- מורה למסנן מערכת הקבצים לתרגם את הזרמים הרבים לזרם בודד, כאשר הקובץ מועבר למערכות קבצים שאינן תומכות ב-NSS.

Disk Quotas

מנהלים יכולים עתה להגביל את שטח הדיסק שמשתמשים צורכים בשרת. **Disk Quotas** (מכסות דיסק) הוא כלי חזק המשמש לניטור וריסון שימוש בשטח הדיסק. מנהלים יכולים לשלוט על גידול האחסון בסביבות מבוזרות. מכסות דיסק, כפי שהן מיושמות על ידי NTFS, משמשות במערכת Windows 2000 על בסיס מחיצה (Per Partition). מכסות דיסק מתוארות ביתר פירוט בפרק 13.

תמיכה ב- Sparse File Support

Sparse files (קבצים מדוללים) מאפשרים לתוכנות ליצור קבצים גדולים מאוד, אך לצרוך שטח דיסק רק כנדרש. NTFS מסירה הקצאה של זרמי נתונים מדוללים (Sparse Data Streams) ומשאירה רק נתונים לא מדוללים (Non-Sparse), להם יש הקצאת מקום. כאשר תוכנה ניגשת לקובץ מדולל, מערכת הקבצים מניבה נתונים מוקצים כנתונים אמיתיים ונתונים לא מוקצים כאפסים.

ניתן להגדיר מאפיין מערכת קבצים מבוקרת-משתמש לניצול פעולת קובץ מדולל במערכת NTFS. בעוד מאפיין קובץ מדולל מוגדר, מערכת הקבצים יכולה להסיר הקצאה מנתונים ממקום כלשהו בקובץ, וכאשר יישום קורא, להניב נתוני אפס לפי טווח במקום לאחסן ולענות עם הנתונים עצמם. API של מערכות קבצים מאפשרות לקובץ להיות מועתק או מגובה כסיביות אמיתיות וכ- Sparse Stream Ranges. התוצאה הסופית היא אחסון וגישה יעילים למערכת הקבצים.

קובץ מדולל כולל מאפיין הגורם לתת-מערכת הקלט/פלט לפענח את נתוני הקובץ בהתבסס על טווחים מוקצים. כל נתון משמעותי או נתון שאינו-אפס מוקצה, בעוד שכל נתון חסר משמעות (מחרוזות נתונים ארוכות המורכבות מאפסים) פשוט אינו מוקצה. בעת שקובץ מדולל נקרא, נתונים מוקצים מוחזרים (נענים) כמאוחסנים, ואילו נתונים שאינם מוקצים, מוחזרים (נענים), כברירת מחדל, כאפסים בהתאם לדרישות בטיחות של תקן C2.

שימוש ב-Sparse File Utilization

NTFS כוללת תמיכה מלאה בקבצי Sparse דחוסים ופרוסים. הקצאת דיסק נדרשת עבור טווחים מוגדרים בלבד. NTFS מטפלת במטלות קריאה של קבצי Sparse על ידי מענה של נתונים מוקצים ונתוני Sparse המוגדרים על ידי טווחי מיפוי קבצים. ניתן לקרוא קובץ Sparse כנתונים מוקצים ונתוני טווח ללא צורך באחזור כל ערכת הנתונים. דבר זה רצוי עבור יישומים הרוצים לטפל בקבצי Sparse באופן יעיל במהלך עבודתם. ברירת המחדל של NTFS היא מענה באמצעות ערכת הנתונים כולה.

לזרמי נתונים עם ערכת מאפייני NTFS מדוללים יש שתי הגדרות הקצאה. הראשונה היא הווירטואלית בשם **AllocatedLength**, המעוגלת עד לגבול אשכול גדול או שווה בגודלו לזרם. השנייה מכונה **TotalAllocatedLength**, המייצגת את אשכולות הדיסק עצמם המוקצים לזרם. TotallAllocatedLength תהיה תמיד קטנה או שווה ל-AllocatedLength.

דוגמה לשימוש בקבצים מדוללים הוא יישום מדעי הדורש שטח אחסון של 1TB עבור נתונים המשמשים במטריצה (Matrix). המידע המשמעותי במטריצה יכול להיות 1MB בלבד. בעזרת ערכת מאפייני קובץ מדולל, מערכת הקבצים יכולה להסיר מההקצאה מכל מקום בקובץ ולהפיק אפס נתונים ליישומים הקוראים את הקובץ לפי טווח, במקום לאחסן ולענות עם הנתונים עצמם. התוצאה היא שדרישות גישה לקובץ מסופקות עם הסיביות הנכונות ושטח הדיסק מנוהל ביעילות. API של מערכות קבצים מאפשרות העתקה או גיבוי הקובץ כסיביות אמיתיות וטווחי זרימה של Sparse. התוצאה הסופית היא יעילות באחסון וגישה למערכת הקבצים.

Link Tracking And Object Identifiers

Windows 2000 מספקת שירות המאפשר ליישומי לקוחות לעקוב אחר מקורות קישורים שהועברו מהמערך המקומי או בתחום. לקוחות המצטרפים כמנויים לשירות מעקב הקישורים יכולים לשמור על שלמות ההפניות שלהם, כיון שהאובייקטים המופנים ניתנים להעברה באופן שקוף. **Link Tracking** (מעקב קישורים) שומר מזהה אובייקט קובץ כחלק מנתוני המעקב שלו. תכונה זו מאפשרת לקיצורי דרך לאתר את הנתיב הנכון של תיקיה או קובץ לאחר שהועברה.

שירות מעקב הקישורים המבוזר שומר על קישורי קבצים אם קובץ מקור הקישור הועבר מ-NTFS version 5.0 volume ל-Volume אחר מאותה גירסה באותו Domain. קשרי קבצים נשמרים גם אם שם המחשב ששומר את מקור הקישור משתנה, או אם שיתופי הרשת במחשב מקור הקישור משתנה, או ה-Volume השומר את קובץ מקור הקישור מועבר למחשב אחר באותו Domain.

Change Journal

Change Journal (יומן שינויים) הוא זרם Sparse היוצר יומן עקבי, למעקב אחר נתוני קובץ המתייחסים לתוספות, מחיקות, ושינויים עבור כל NTFS volume. דבר זה יעיל ליישומים הדורשים לדעת מה אירע ב-volume מסויים. אינדקסים של מערכות קבצים, מנהלי שכפול, אחסון מרוחק ויישומי גיבוי מצטברים (Incremental), הם מקצת מהדוגמאות ליישומים שיכולים ליהנות מיומן השינויים.

עם יומן השינויים, רק קטע פעיל קטן של הקובץ משתמש בהקצאת דיסק. הטווח הפעיל מתחיל בהיסט 0 בזרם ונע קדימה בתוך הקובץ. **U**nique **S**equence **N**umber (USN, מספר סדרתי ייחודי) של רשומה מסוימת מייצג את ההיסט הוירטואלי שלה בזרם. ככל שהטווח הפעיל נע קדימה בזרם, רשומות קודמות מוסרות מההקצאה והופכות בלתי זמינות. ניתן לכוון את גודל הטווח הפעיל בקובץ מדולל.

יומן השינויים יעיל בהרבה מחותמות זמן או ציוני קבצים למעקב שינויים בשטח שם נתון. מנהל המערכת יכול לעיין בשינויים שנעשו ב-Volumes ללא מעבר על טווחי שמות.

מודעות Change Journal

יומן השינויים לא ישפיע על יישום אחסון אלא אם היישום עושה בו שימוש מוגדר. יומן השינויים פועל בשטח domain. הוא מבוסס על זרם נתוני Sparse המאפשר הסרה מהקצאה מקדמת הקובץ. אי לכך, ניתן להסיר רישומי שינויים וכל יישום התלוי ברישומים אלה, חייב להיות ערוך לטפל באירוע זה. יומן השינויים רושם נתונים לפי Volume. הוא ישים רק עבור NTFS Volumes .

Unique Sequence Number

יומן USN (**U**nique **S**equence **N**umber Journal) מספק יומן עקבי של כל השינויים שנעשו לקבצים ב-Volume. יישומים יכולים להיוועץ ביומן USN לקבלת נתונים על שינויים שנעשו לקבוצת קבצים. יומן USN יעיל יותר מבדיקת חותמות זמן או רישום של ציוני קבצים.

כאשר משתמש, Administrator, או Domain Controller אחר מעדכן אובייקט ספריית רשת, משייך בקר אובייקט ספריית הרשת מספר USN לשינוי. כל DC שומר על USN של עצמו ומיישם כל אחד בצורה סדרתית לכל שינוי ספריית הרשת שנעשה בספריית הרשת שלו. בנוסף, כל DC שומר טבלאות USN שקיבל מכל ה-DCs שב-domain.

כאשר DC כותב את השינוי בספריית הרשת, הוא כותב גם את ה-USN של השינוי עם התכונה. זו היא פעולה אוטומטית (הליך הפועל כהליך אחיד בלתי ניתן לחלוקה), כך שכאשר ה-DC כותב את שינוי התכונה ואת ה-USN של השינוי, או שהוא יצליח לחלוטין או שייכשל לחלוטין.

תמיכה ב-CD ו-DVD

Windows 2000 תומכת בהתקני אחסון CDFS, UDF ו-DVD.

מערכת קבצים לתקליטור - CDFS

Windows 2000 ממשיכה לספק תמיכת קריאה-בלבד עבור CDFS (**CD**-ROM **F**ile **S**ystem), שהיא תואמת תקן ISO 9660. כמו כן, Windows 2000 תומכת גם בשמות קבצים הערוכים לפי תקן ISO 9660 Level 2.

בעת יצירת תקליטור שישמש במערכת הפעלה Windows 2000, הקפד על התקנים הבאים:

- כל שמות התיקיות והקבצים חייבים להיות בני פחות מ- 32 תווים.
- עץ התיקיות אינו יכול להכיל יותר משמונה רמות מתחת לשורש.
- אין חובה להשתמש בסיומות קבצים.

הערה CDFS אינו תומך בשמות קבצים באותיות קטנות. כאשר נעשה ניסיון לגשת לשם קובץ או ספריה על ידי תקליטור על ידי כתיבה באות קטנה, תתקבל הודעת שגיאה File Not Found (הקובץ לא נמצא).

(**U**niversal **D**isk **F**ormat) UDF

מערכת קבצים UDF, שהיא חדשה עבור Windows 2000, היא מערכת קבצים שתוכננה לתעבורת נתונים על DVD ותקליטורים. הייעוד העיקרי של UDF הוא תמיכה במדיה של DVD-ROM. UDF היא מערכת קבצים מבוססת-תקן התואמת לתקן ISO 13346.

הטבלה להלן מפרטת את המגבלות והדרישות של מפרט UDF :

פריט	דרישה
גודל סקטור לוגי/פיסי	הגודל הלוגי והפיסי עבור Volume נתון יהיה זהה.
גודל בלוק לוגי	הגודל הלוגי של בלוק עבור logical volume יותאם לגודל הלוגי של סקטור ה-Volume.
Volume Set Physical Sector Size	הגודל הפיסי של כל המדיה באותה ערכת volumes יהיה בעל גודל סקטור פיסי זהה.

עם UDF, תמיכה ב-MultiVolume היא אופציונלית. תמיכה במדיה מוגבלת ל-Rewrite (כתיבה חוזרת), Overwrite (דריסה), ו-**W**rite **O**nce, **R**ead **M**any (WORM, כתיבה חד-פעמית, קריאה רב-פעמית). Windows 2000 מספקת תמיכה מקומית לקריאה בלבד עבור UDF. יכולות שכתוב, כתיבה חוזרת ו-WORM מסופקות על ידי יישומי צד שלישי בלבד.

תמיכה ב-DVD

אחד מהתקני האחסון החדשים הנתמכים על ידי Windows 2000 הוא DVD. ל-DVD יש קיבול של כמעט פי 20 מתקליטור רגיל, כך שמשתמש יכול לאחסן מספר מצגות וידיאו עבור מצגת לקוח ועדיין יישאר לו מקום לחומר נוסף.

התמיכה ב-DVD על ידי Microsoft אינה מוגבלת למנהל התקן לתמיכה בכונני DVD-ROM בלבד. כיון ש-DVD כולל טווח רחב ביותר של שימושים וטכנולוגיות, יש לראות את DVD בהקשר של המחשב כולו. דיסקים של DVD והתקנים מהווים מדיית אחסון כלכלית עבור קבצי נתונים גדולים. בעתיד, DVD יכלול גם אמצעי כתיבה ובכך יאפשר טווח אפשרויות רחב יותר.

הערה הספריה **M**icrosoft **S**olution **D**eveloper **N**etwork (MSDN) זמינה עתה על תקליטור DVD.

ברוב המחשבים הכוללים תמיכת DVD של Microsoft, יתפקד DVD כאמצעי אחסון, ואם מותקנת גם חומרת פענוח כנדרש, היא תתמוך באחזור והשמעת DVD מלא.

חלק מהרכיבים ישתנו בהתבסס על התקדמות טכנולוגית של חומרה אחרת, כגון כניסתה של טכנולוגיית **A**ccelerated **G**raphics **P**ort - AGP, או שיפורים באפיק PCI. הרכיבים היחידים שיהיו קיימים תמיד הם מנהלי התקן תקליטור DVD, מערכת קבצים UDF, **W**indows **D**river **M**odel (WDM) ו- DVD Splitter/Navigator.

מנהל התקן בעל סיווג תקליטור DVD
(DVD-ROM Class Driver)

לתקליטורי DVD יש ערכת פקודות בעלת תקן מוגדר. תמיכה בערכת פקודות זו מסופקת ב-Windows 98 על ידי מנהל התקן מעודכן בסיווג (Class) תקליטורים. ב-Windows 2000 התמיכה מסופקת על ידי מנהל התקנים חדש - WDM DVD-ROM. מנהל ההתקן של Windows 2000 מספק יכולת קריאה של סקטורים של נתונים מכונן תקליטור DVD.

תמיכה ב-UDF מסופקת לאבטחת תמיכה לדיסקים DVD, שפורמטו בשיטת UDF. Windows 2000 תספק מערכות קבצים ניתנות להתקנה מסוג UDF הדומים ל-FAT16 ו-FAT32.

הגנת זכויות העתקה (Copyright)

הגנת זכויות העתקה ב-DVD מסופקת על ידי הצפנת סקטורים חשובים על הדיסק ואז פענוח סקטורים אלה לפני קריאתם. Microsoft תספק מפענחים מבוססי תוכנה וחומרה על ידי שימוש בערכת תוכנה, שתאפשר אימות בין מפענחים לכוננים של תקליטורי DVD במחשב.

חלוקה לאזורים

כחלק מתוכנית הגנת זכויות העתקה עבור DVD, הוקמו ששה אזורים עולמיים על ידי איגוד ה-DVD. ניתן לאחזר מידע מתקליטורי DVD בחלק או בכל האזורים, בהתאם לקוד אזורי שהוגדר על ידי מפיקי תוכן עבור DVD. Microsoft תספק תוכנה שתגיב לקודים אזוריים, כפי שיידרש על ידי איגוד DVD וכחלק מרשיונות הפענות.

מבנה NTFS

חלק זה דן ברכיבים העיקריים של מבנה NTFS : מבנה NTFS Volumes, סקטור האתחול של Windows 2000, טבלת קבצים עיקרית (Master File Table) ו-Metadata של Windows 2000, ומאפייני קבצים של NTFS.

מבנה NTFS Volumes

NTFS משתמש ב-Clusters (אשכולות) (הידועים גם כיחידות הקצאה) הבנויים מסקטור אחד או יותר כיחידה הבסיסית של הקצאת שטח דיסק. אולם, גודל ברירת המחדל של האשכול תלוי בגודל המחיצה. בתוסף התוכנה Disk Management, המשתמש יכול להגדיר גודל אשכול של עד 4KB (4096 בתים). אם נעשה שימוש בתוכנת Format.exe דרך מנחה הפקודה לצורך פרמוט NTFS volume, המשתמש יכול להגדיר אשכול באחד הגדלים המופיעים בטבלה להלן.

אזהרה דחיסת NTFS אינה נתמכת עבור אשכולות הגדולים מ- 4KB.

גודל Volume	סקטורים בכל אשכול	גודל האשכול
512MB או פחות	1	512 בתים
513MB-1024MB	2	1KB
1025MB-2048MB	4	2KB
2049MB-4096MB	8	4KB
4097MB-8192MB	16	8KB
8193MB-16,384MB	32	16KB
16,385MB-32,768MB	64	32KB
>32,768MB	128	64KB

גדלי האשכולות בטבלה זו הם המלצה בלבד. ניתן לשנות את הגדלים, אם נדרש. אולם, שינוי מימדי אשכול דורש פרמוט מחדש של המחיצות.

סקטור האתחול של Windows 2000

הנתון הראשון המופיע ב-NTFS VolumeS הוא סקטור האתחול. סקטור האתחול מתחיל בסקטור 0 ואורכו יכול להגיע עד 16 סקטורים. הוא מורכב משני מבנים:

- בלוק פרמטר ה-BIOS, הכולל נתונים אודות מבנה ה-Volume ומבנה מערכת הקבצים.
- קוד המתאר כיצד לאתר ולטעון את קבצי האתחול עבור מערכת ההפעלה הנטענת. עבור Windows 2000 במחשבים מבוססי מעבד x86, קוד זה טוען את הקובץ Ntldr.

MFT ו-Metadata של Windows 2000

כאשר volume מפורמט NTFS, טבלת **M**aster **F**ile **T**able (MFT), טבלת קובץ אב) ו-Metadata נוצרים.

NTFS משתמשת ברישומי MFT להגדרת הקבצים שמתייחסים אליהם. כל נתוני הקובץ, כולל גודלו, חותמות זמן ותאריך, הרשאות ותכולת נתונים מאוחסנים או ברשומות MFT או בשטח חיצוני ל-MFT אך מתואר על ידי רישומי MFT.

NTFS יוצרת רשומת קובץ עבור כל קובץ, ורשומת ספריה עבור כל ספריה הנוצרת ב- NTFS volume. MFT כולל קובץ רשומה נפרד עבור MFT עצמו. רשומות קבצים

ותיקיות אלו מאוחסנות ב-MFT. NTFS מקצה שטח עבור כל רשומת MFT, בהתבסס על גודל אשכול הקובץ. מאפייני הקובץ נכתבים לשטח המוקצה ב-MFT. פרט למאפייני הקובץ, כל רשומת קובץ מכילה נתונים על מיקום רשומת הקובץ ב-MFT.

בדרך כלל, לכל קובץ יש רשומת קובץ אחת. אולם, אם לקובץ יש מספר רב של מאפיינים או שהוא מתפצל לחלקים רבים (Fragmented), הוא עלול להידרש ליותר מרשומת קובץ אחת. במקרה כזה, הרשומה הראשונה של הקובץ (רשומת הבסיס של הקובץ) מאחסנת את מיקום שאר רשומות הקובץ הנדרשים על ידי הקובץ. קבצים וספריות קטנות (1,500 בתים או פחות) נכללים בשלמותם ברשומת MFT של הקובץ.

Metadata הם הקבצים המשמשים את NTFS ליישום מבנה הקבצים. NTFS שומרת את 16 הרשומות הראשונות של MFT עבור Metadata (1MB בקירוב). הרשומות הנותרות של MFT מכילים את רשומות הקבצים והספריות עבור כל קובץ וספריה במחיצה.

אם רשומת MFT נהרסת, קוראת NTFS את הרשומה השנייה, לאיתור קובץ השיקוף של MFT. מיקומי קטע הנתונים עבור $Mft ו- $MftMirr נרשמים בסקטור האתחול. העתק של סקטור האתחול נמצא בקצה המחיצה.

מאפייני קבצים של NTFS

כל סקטור מוקצה במחיצת NTFS שייך לקובץ. אפילו Metadata של מערכת הקבצים היא חלק מקובץ. NTFS רואה כל קובץ (או תיקיה) כערכת מאפייני קובץ. רכיבים כמו שם הקובץ, נתוני האבטחה שלו ואף נתוניו, הם כולם מאפייני קובץ.

קוד סוג המאפיין, ואפשרי גם שם המאפיין, מזהים כל מאפיין. כאשר ניתן להכיל את מאפייני הקובץ ברשומת קובץ MFT עבור קובץ זה, הם נקראים **Resident Attributes** (מאפיינים מאוכלסים). נתוני שם הקובץ וחתימת הזמן הם תמיד מאפיינים מאוכלסים. כאשר המידע של קובץ גדול מדי להיכלל בקובץ רשומת MFT, חלק ממאפייני הקובץ אינם מאוכלסים. למאפיינים לא מאוכלסים מוקצה אשכול אחד או יותר של שטח דיסק במקום אחר ב-Volume. NTFS יוצרת מאפיין של רשימת מאפיינים לציון מיקום של כל רשומות המאפיינים.

יישום NTFS

בעת יישום NTFS, יש לקחת בחשבון מספר גורמים: שדרוג ל-Windows 2000, אתחול-מרובה (Multiboot) של Windows 2000, ונושאי תאימות NTFS.

שדרוג ל- Windows 2000

שדרוג מ-Windows NT ל-Windows 2000 (כאשר לא נדרש אתחול כפול) יוצר תוצאות כדלקמן:

- ❖ כל ה-Volumes שפורמטו בעבר עם גירסה קודמת של NTFS, ישודרגו ל-NTFS גירסה 5.0.
- ❖ כל boot/system volume שפורמט עם FAT16 יוסב ל-NTFS גירסה 5.0.
- ❖ כל Volume שפורמט עם FAT16 שאינו boot/system volume אינו מוסב.

חבילת שירות גירסה 4 (SP4) או מאוחרת יותר עבור Windows NT 4.0

כאשר Windows 2000 מותקנת (לא משדרגת) על מחשב המפעיל Windows NT 4.0, כל ה-NTFS volumes, שפורמטו בעבר עם גרסה קודמת של NTFS, ישודרגו אוטומטית ל-NTFS גירסה 5.0. כדי שמערכת Windows NT 4.0 תוכל לגשת לכל ה-Volumes (או אף לאתחל), עלינו להתקין על מערכת Windows NT 4.0 את חבילת השירות גירסה 4 (service pack 4.0) או מאוחרת יותר.

הסבת FAT Volume

הסבה מ-FAT ל-NTFS מתרחשת רק אם המשתמש מאשר אותה. לאחר הפעלת תוכנית ההתקנה Winnt32.exe במצב Attend (מאויש), היא תציג מסך הסבת מערכת קבצים המאפשר למשתמש להסב את מערכת קבצי FAT הנוכחית למערכת NTFS. התקנות או שדרוגים באמצעות Winnt32.exe שביצועם חל במצב Unattend (לא מאויש, אוטומטי), יסבו או לא יסבו את מערכת הקבצים בהתבסס על הערכים המופיעים בשם ערך של FileSystem שבקובץ התשובות. הסבה תתרחש אוטומטית אם FileSystem=ConvertNTFS, ולא תתרחש אם FileSystem=LeaveAlone. בעת התקנת Windows 2000 Server, ברירת המחדל של האפשרות להסב FAT ל-NTFS תהיה Yes. אם שם ערך FileSystem אינו קיים, תוכנית ההתקנה לא תסב את מערכת הקבצים ולא תטפל בה.

אם המשתמש מפעיל את תוכנית ההתקנה באמצעות Winnt32.exe, דיסקטים לאתחול, או תקליטור אתחול, מצב טקסט של הליך ההתקנה מאפשר למשתמש לבחור במערכת הקבצים הרצויה.

הטבלה להלן סוקרת את נתוני הסבת מערכת הקבצים.

מערכת	FAT ל-NTFS	NTFS ל-NTFS 5.0
תחנת עבודה Windows NT 3.51	Winnt32.exe יציג את עמוד האשף ובו נבחר מצב No Option (ללא אופציות).	כל ה- NTFS volumes הטעונים ישודרגו למערכת NTFS גירסה 5.0. תוצג אזהרה, והמשתמש יוכל לבטל את תוכנית ההתקנה או להמשיך ולהתקדם.
Windows NT 3.51 Server (Standalone/DC)	Winnt32.exe יציג את עמוד האשף ובו נבחר מצב Yes Option (עם אופציות).	כל ה-NTFS volumes הטעונים ישודרגו למערכת NTFS גירסה 5.0. תוצג אזהרה, והמשתמש יוכל לבטל את תוכנית ההתקנה או להמשיך ולהתקדם.
תחנת עבודה Windows NT 4.0 (גירסה קודמת ל-SP3)	Winnt32.exe יציג את עמוד האשף ובו נבחר מצב No Option (ללא אופציות).	כל ה-NTFS volumes הטעונים ישודרגו למערכת NTFS גירסה 5.0. תוצג אזהרה, והמשתמש יוכל לבטל את תוכנית ההתקנה או להמשיך ולהתקדם.
תחנת עבודה Windows NT 4.0 (SP3)	Winnt32.exe יציג את עמוד האשף ובו נבחר מצב No Option (ללא אופציות).	כל ה-NTFS volumes הטעונים ישודרגו למערכת NTFS גירסה 5.0. תוצג אזהרה, והמשתמש יוכל לבטל את תוכנית ההתקנה או להמשיך ולהתקדם.
תחנת עבודה Windows NT 4.0 (SP4 או מאוחרת יותר)	Winnt32.exe יציג את עמוד האשף ובו נבחר מצב No Option (ללא אופציות).	כל ה-NTFS volumes הטעונים ישודרגו למערכת NTFS גירסה 5.0.
Windows NT 4.0 Server (גירסה קודמת ל- SP3 - DC/Standalone)	Winnt32.exe יציג את עמוד האשף ובו נבחר מצב Yes Option (עם אופציות).	כל ה-NTFS volumes הטעונים ישודרגו למערכת NTFS המשמשת ב-Windows 2000. תוצג אזהרה, והמשתמש יוכל לבטל את תוכנית ההתקנה או להמשיך ולהתקדם.

מערכת	FAT ל-NTFS	NTFS ל-NTFS 5.0
Windows NT 4.0 Server (גרסת SP3 - DC/Standalone)	Winnt32.exe יציג את עמוד האשף ובו נבחר מצב Yes Option (עם אופציות).	כל ה-NTFS volumes הטעונים ישודרגו למערכת NTFS גירסה 5.0. תוצג אזהרה, והמשתמש יוכל לבטל את תוכנית ההתקנה או להמשיך ולהתקדם.
Windows NT 4.0 Server (גירסה SP4 או מאוחרת יותר - DC/Standalone)	Winnt32.exe יציג את עמוד האשף ובו נבחר מצב Yes Option (עם אופציות).	כל ה-NTFS volumes הטעונים ישודרגו למערכת NTFS גירסה 5.0.
Windows 95	לא תבוצע כל הסבה. מערכת הקבצים תישאר שלמה.	לא ישים - לא מתבצעת הסבה
Windows 95 OSR2	לא תבוצע כל הסבה. מערכת הקבצים תישאר שלמה.	לא ישים - לא מתבצעת הסבה
Windows 98	לא תבוצע כל הסבה. מערכת הקבצים תישאר שלמה.	לא ישים - לא מתבצעת הסבה

לאחר סיום התקנה, ניתן להסב מחיצת FAT ל-NTFS על ידי פקודת Convert מתוך שורת הפקודות :

convert *volume* /FS:NTFS /V

המילה volume תוחלף בשם הכונן, והאפשרות /V משמעותה : הפקודה תרוץ במצב Verbose. למשל :

convert C: /FS:NTFS /V

Multibooting Windows 2000

יכולת הגישה ל-NTFS volumes כאשר המשתמש מיישם Multibooting Windows 2000 יחד עם אתחול גרסאות קודמות של Windows NT, תלוי בגרסת Windows NT שבשימוש.

אם משתמש מאתחל עם מערכת Windows NT 4.0 SP4, ניתן לקרוא כל basic volume (לא דינמי) המפורמט עם NTFS גירסה 5.0.

אם משתמש מאתחל עם מערכת Windows NT הקודמת לגרסת Windows NT 4.0 SP4, לא ניתן יהיה לגשת למחיצות NTFS.

תאימות NTFS

אם משתמש מפעיל מערכת Windows NT 4.0 SP4, כל basic volume (לא דינמי) המפורמט עם NTFS המשמש ב-Windows 2000, ניתן לקריאה.

מנהל התקן NTFS של Windows NT 4.0 SP4, מאפשר למשתמשי Windows NT 4.0 לטעון volumes שפורמטו עם NTFS 5.0. אולם, משתמשי Windows NT 4.0 לא יוכלו לנצל את התכונות החדשות של NTFS 5.0.

רק מערכות Windows 2000 ו-Windows NT 4.0 SP4 מאפשרות גישה לנתונים ב-NTFS version 5.0 Volumes. לפיכך, אם קיימת מערכת הפעלה אחרת במחשב Multibooting Windows 2000, יש לפרמט את מחיצת המערכת והאתחול של המערכת השונה, בפורמט שאינו NTFS (כגון FAT16 או FAT32).

Ntfs.sys File System Driver

מנהל ההתקן Ntfs.sys של Windows NT 4.0 מספק תמיכה לטעינת volumes ומערכות Multiboot בסביבה מעורבת של מערכות מסוג Windows NT. עקב בעיות תאימות אלו, לא מומלץ לבצע אתחול כפול בין Windows NT 4.0 ל-Windows 2000. מנהל התקן Windows NT 4.0 SP4 NTFS קיים רק לסייע בהערכה ושדרוג ל-Windows 2000.

Mounting Volumes

התקנת Windows 2000 משדרגת מחיצות NTFS 4.0 באופן אוטומטי ל-NTFS גירסה 5.0. אם מחיצת האתחול של Windows NT 4.0 היתה בפורמט NTFS ולא הותקן service pack 4.0, לא ניתן יהיה לאתחל את המחשב למערכת Windows NT 4.0. מערכת Windows NT 4.0 SP4 יכולה לאתחל ממחיצת NTFS ולגשת לנתונים בכל המחיצות בפורמט NTFS (בדיסק בסיסי), אך אינה יכולה לנצל את התכונות החדשות (כגון הצפנה) של מערכת הקבצים NTFS 5.0.

Dual-Boot Systems

מנהל ההתקן החדש של מערכת קבצים NTFS (הנמצא בחבילת שירות גירסה 4.0 ומעלה) מאפשר לבצע אתחול בין מערכות Windows NT 4.0 ל-Windows 2000. לאתחול כפול של Windows NT 4.0 ו-Windows 2000, יש להתקין את SP4 על מערכת Windows NT 4.0. אולם, כיון שמבנה הנתונים על הדיסק של NTFS שונה תחת מערכת ההפעלה Windows 2000, תוכניות שירות דיסק של Windows NT 4.0 כגון CHKDSK ו- AUTOCHK לא יפעלו. תוכניות שירות אלה בודקות את חותמת הגירסה של מערכת ההפעלה לפני ביצוע משימותיהן.

לאחר התקנת Windows 2000, על המשתמש להפעיל תוכניות שירות של הדיסק אשר נכתבו למערכת Windows 2000.

אף שהתכונות אינן זמינות בעת טעינת NTFS 5.0 volume תחת Windows NT 4.0 SP4, ניתן לבצע את רוב פעולות הכתיבה והקריאה כרגיל אם פעולות אלה אינן נדרשות לתכונות של NTFS 5.0.

כיון שניתן לקרוא ולכתוב קבצים על NTFS 5.0 volumes תחת Windows NT 4.0, ייתכן שמערכת Windows 2000 תצטרך לבצע פעולות ניקוי על ה-volume לאחר שתיטען על Windows NT 4.0. הניקוי מוודא שמבנה נתוני NTFS 5.0 נשמרו אחידים לאחר טעינת Windows NT 4.0.

Disk Quotas

בעת הפעלת Windows NT 4.0 אין התייחסות למכסות דיסק של Windows 2000. המשמעות היא שמשתמשים יכולים להשתמש ביותר שטח דיסק מהמכסה המוגדרת להם ב-Windows 2000.

אם משתמשים תחת Windows NT 4.0 חורגים מהמכסות שהוקצו להם ב-Windows 2000, הרי שבהפעלת Windows 2000 תסרב המערכת להקצות למשתמשים אלה שטח דיסק נוסף. משתמשים יכולים עדיין לכתוב ולקרוא נתונים לקבצים קיימים, אך אינם יכולים להגדיל את הקובץ. אולם, הם יכולים למחוק קבצים ולכווץ קבצים קיימים. התנהגות זו נמשכת עד שהמשתמש יוריד את צריכת שטח הדיסק שלו אל מתחת למכסה שהוקצתה לו. אם הגיע מתחת למכסה שלו, הוא מוחזר להתנהגות מכסות רגילה.

הערה זוהי התנהגות רגילה של מכסות כאשר מערכת המכסות מועברת ממצב מעקב או אי-מעקב למצב אכיפה. התנהגות זו תשוב ותופיע כאשר מערכת משודרגת מ-Windows NT 4.0 ל-Windows 2000, בה יש סביבת אכיפת מכסות.

הצפנה

קבצים שהוצפנו (Encrypted) במערכת Windows 2000, לא ניתן לבצע עליהם שום פעולה, כולל פתיחה, קריאה, כתיבה, העתקה ומחיקה תחת מערכת Windows NT 4.0. כיון שלא ניתן לגשת לקבצים מוצפנים תחת Windows NT 4.0, אין צורך בפעולות ניקוי תחת Windows 2000.

Sparse Files

לא ניתן לבצע שום פעולה, כולל פתיחה, קריאה, כתיבה, העתקה ומחיקה, על קבצי Sparse תחת מערכת Windows NT 4.0. כיון שלא ניתן לגשת לקבצי Sparse תחת Windows NT 4.0, אין צורך בפעולות ניקוי תחת Windows 2000.

Object Ids

יש גישה מלאה לאובייקטים תחת Windows NT 4.0. ניתן לפתוח, לקרוא, לכתוב, להעתיק ולמחוק אובייקטים. אם משתמש מחק קובץ עם מזהה אובייקט זיהוי עליו, Windows 2000 חייבת לסרוק ולנקות את הרישומים היתומים.

USN Journal

Windows NT 4.0 מתעלמת מיומן USN. לא מתבצע כל רישום בעת גישה לקבצים. כיון שכך, לא כל שינוי בקבצים נאגר ביומן USN. כאשר Windows 2000 מאתחלת, הפרמטרים של יומן USN מאופסים כדי לציין שההיסטוריה של היומן אינה שלמה. יישומים המסתייעים ביומן USN צריכים להגיב בהתאם ליומנים לא שלמים. כל גישה נוספת תחת Windows 2000 תירשם, וניתן לסמוך על היומן לאחר טעינת ה-volume על ידי Windows 2000. שים לב שניתן לבצע שאילתת יומן עבור טווחי USN.

Reparse Points

לא ניתן לבצע שום פעולה, כולל פתיחה, קריאה, כתיבה, העתקה ומחיקה, על נקודות Reparse תחת מערכת Windows NT 4.0. כיון שלא ניתן לגשת לנקודות Reparse תחת Windows NT 4.0, אין צורך בפעולות ניקוי תחת Windows 2000.

סיכום שיעור

NTFS 5.0 תומכת בכל התכונות של מערכת ההפעלה Windows 2000, כולל נקודות Reparse, NSS ומכסות דיסקים. NTFS תומכת גם במערכת קבצים לתקליטורים (CDFS), בפורמט דיסק אוניברסלי (UDF) ובהתקני אחסון של DVD. NTFS משתמשת בסקטורים הבנויים מאשכולות רבים כיחידה הבסיסית של הקצאת שטח דיסק. אולם, עם NTFS, גודל ברירת המחדל של האשכול תלוי בגודל המחיצה. פריט המידע הראשון הנמצא על מחיצת NTFS הוא סקטור האתחול. סקטור האתחול מתחיל בסקטור 0 ואורכו יכול להגיע עד סקטור 16. כאשר Volume מפורמט עם NTFS, נוצרים MFT ו- Metadata. כל סקטור מוקצה ב-volume NTFS שייך לקובץ. אפילו מערכת הקבצים Metadata היא חלק מקובץ. NTFS רואה כל קובץ (או תיקיה) כערכת מאפייני קובץ. בעת החלת NTFS, יש לקחת מספר גורמים בחשבון: שדרוג ל-Windows 2000, Multibooting ב-Windows 2000 ונושאי תאימות NTFS.

שיעור 4: אבטחת מערכות קבצים

פעולת שיתוף, היא הדרך היחידה לגרום לכך שתיקיות ותוכנן יהיו זמינים ברשת. תיקיות משותפות מאפשרות אבטחת משאבים; ניתן להשתמש בהן במחיצות FAT16 ו-FAT32, כמו גם במחיצות NTFS. אך NTFS תומכת ביותר מתיקיות משותפות בלבד. הרשאות NTFS משמשות להגדרת המשתמשים והקבוצות שיכולים לגשת לקבצים ותיקיות, ומה מותר להם לעשות בתוכנם. אולם, הרשאות NTFS אינן זמינות ב-Volumes שפורמטו עם FAT.

לאחר שיעור זה, תוכל

- לשתף תיקיות ולהקצות הרשאות לשיתופים אלה.
- להקצות הרשאות NTFS לקבצים ותיקיות.

זמן לימוד משוער: 35 דקות

תיקיות משותפות

תיקיות משותפות מאפשרות למשתמשים ברשת גישה למשאבי קבצים. כאשר תיקיה משותפת, משתמשים יכולים להתחבר לתיקיה באמצעות הרשת ולגשת לקבצים שבתוכה. אולם, לקבלת גישה לקבצים אלה, נדרש שלמשתמשים יהיו הרשאות מתאימות לגשת לתיקיות המשותפות.

הרשאות עבור תיקיות משותפות

תיקיה משותפת עשויה להכיל יישומים, נתונים או מידע אישי של משתמשים (הנקראים בשם תיקיות בית). כל סוג נתון עשוי לדרוש הרשאה שונה בתיקיה המשותפת.

להרשאות תיקיות משותפות ישנן תכונות המשותפות:

- הרשאות עבור תיקיות משותפות חלות על תיקיות, לא על קבצים בודדים. כיון שניתן להחיל הרשאות לתיקיות משותפות רק לתיקיה המשותפת כולה ולא לקבצים בודדים או תת תיקיות שבתוך התיקיה המשותפת, הרשאות עבור תיקיות משותפות מספקות אבטחה פרטנית פחות מהרשאות NTFS.
- הרשאות תיקיות משותפות אינן מגבילות גישה למשתמשים הניגשים לתיקיה במחשב המקומי שבו התיקיה מאוחסנת, כאשר הם יושבים פיזית מול המחשב. ההרשאות חלות רק על משתמשים המתחברים לתיקיה דרך הרשת.
- הרשאות עבור תיקיות משותפות הן הדרך היחידה לאבטחת משאבי רשת ב-FAT volume. הרשאות NTFS אינן זמינות ב-FAT volumes.

- הרשאת ברירת המחדל בתיקיה משותפת היא Full Control (שליטה מלאה), והיא מוחלת על קבוצת Everyone (כולם) בעת שיתוף הקובץ.

תיקיה משותפת מופיעה בסייר Windows כסמל של יד האוחזת בתיקיה המשותפת (תרשים 4.9).



תרשים 4.9 התיקיה download משותפת בסייר Windows.

כדי לשלוט בגישת משתמשים לתיקיות משותפות, עליך להקצות הרשאות לתיקיות המשותפות. הטבלה להלן מפרטת מה ניתן לבצע עם כל הרשאה. ההרשאות מסודרות מהמגבילות ביותר למגבילות פחות.

הרשאה	תיאור
Read (קריאה)	משתמשים יכולים להציג שמות תיקיות, שמות קבצים, נתוני קבצים ומאפיינים; הם יכולים להפעיל קבצי תוכנות, ולעבור בין התיקיות בתיקיה המשותפת.
Change (שינוי)	משתמשים יכולים ליצור תיקיות, להוסיף קבצים לתיקיות, לשנות מאפייני קבצים, למחוק תיקיות וקבצים, ולבצע פעילות מורשית על ידי הרשאת **קריאה**.
Full Controll (שליטה מלאה)	משתמשים יכולים לשנות הרשאות קבצים, לקחת בעלות על קבצים, ולבצע את כל הפעילות המורשית על ידי הרשאת **שינוי**.

ניתן לאפשר (Allow) או למנוע הרשאות (Deny) בתיקיה משותפת למשתמשים בודדים או קבוצות משתמשים. ככלל, מוטב להקצות הרשאות לקבוצה ולא למשתמשים בודדים. עליך למנוע הרשאות (Deny) רק כאשר יש צורך למנוע הרשאה המיושמת בדרך כלל. לדוגמה, ייתכן שיהיה צורך למנוע הרשאה ממשתמש כלשהו השייך לקבוצה שקיבלה הרשאות. אם תמנע הרשאת תיקיה משותפת מהמשתמש, למשתמש לא תהיה הרשאה זו.

לדוגמה: שיתפת את תיקיית Download והענקת הרשאות Allow מסוג Change לקבוצת משתמשים בשם Users. משתמש בשם User1 שייך לקבוצת Users ולמרות שאינך מעוניין להוציא את המשתמש מהקבוצה, אתה כן מעוניין להגביל אותו להרשאת Read בלבד עבור שיתוף Download. במקרה זה עליך להוסיף את חשבון User1 במפורש לרשימת בעלי ההרשאות עבור שיתוף Download, להעניק לו הרשאת Read ולמנוע ממנו הרשאת Change.

החלת הרשאות תיקיה משותפת

החלת הרשאות שיתוף לחשבונות משתמשים וקבוצות משפיעה על הגישה לתיקיה משותפת. מניעת הרשאה מקבלת עדיפות על פני הרשאות שאפשרת.

הרשאות רבות

משתמש יכול להיות חבר במספר קבוצות, שלכל אחת מהן הרשאות שונות המאפשרות רמות שונות של גישה לתיקיה משותפת. כאשר אתה מקצה הרשאה למשתמש לגישה לתיקיה משותפת ומשתמש זה הוא חבר בקבוצה שלה הקצת הרשאה שונה, ההרשאות המעשיות של המשתמש הן שילוב (Cumulative) ההרשאות האישיות שלו עם אלו של הקבוצה. לדוגמה, אם למשתמש יש הרשאת קריאה והוא חבר בקבוצה שלה הרשאת שינוי, ההרשאה המעשית של המשתמש היא שינוי, הכוללת קריאה. ובאופן כללי, ניתן לומר כי אם יש "התנגשות" בין מספר הרשאות תיקיה, ההרשאה הכי פחות מגבילה היא המעשית.

מניעה גוברת על הרשאות אחרות

מניעה (Deny) מקבלת עדיפות על פני הרשאות אחרות, הניתנות בדרך כלל לחשבונות משתמשים וקבוצות. אם תמנע הרשאת תיקיה משותפת ממשתמש, למשתמש לא תהיה הרשאה זו, אף אם אפשרת הרשאה זו לקבוצה בה המשתמש חבר. מניעה תמיד "מנצחת" הרשאה.

הרשאות NTFS

הרשאות תיקיה משותפת מספיקות לקבלת נגישות לקבצים ותיקיות ב-FAT volume אך אינן הפתרון הטוב ביותר למחיצת NTFS. במחיצת FAT, משתמשים יכולים לקבל גישה לתיקיה משותפת בה יש להם הרשאות, בנוסף לתוכן התיקיה. הרשאות NTFS עדיפות, כיון שניתן להגדיר הרשאות על תיקיות וקבצים גם יחד, וכמו כן, הרשאות NTFS משפיעות באופן מקומי על המשתמש היושב פיסית מול המחשב. אם הוגדרו שיתוף זכויות עבור תיקיה והרשאות NTFS מוגדרות לתיקיות או קבצים בתיקיה, ההרשאות המגבילות ביותר תהינה ההרשאות המעשיות למשאב. דבר זה מגדיל משמעותית את מורכבות הענקת הרשאות למשאבי הרשת. במידה והרשאת NTFS והרשאות שיתוף מתנגשות, אז ההרשאה המגבילה ביותר היא המעשית.

לדוגמה: הענקת הרשאת שיתוף Change לקבוצת Users עבור תיקיית שיתוף Download, ולתיקיה זו יש הרשאת Read NTFS בלבד עבור אותה קבוצת משתמשים. ההרשאה המעשית למשתמשים הניגשים לשיתוף Download דרך הרשת, תהיה הרשאת Read (המגבילה ביותר).

העתקה או העברת תיקיות משותפות

בעת העתקת תיקיה משותפת, התיקיה המקורית עדיין משותפת, אך ההעתק אינו משותף. בעת העברת תיקיה משותפת, היא אינה משותפת יותר.

הנחיות להרשאות תיקיה משותפת

הרשימה הבאה מספקת מספר הנחיות כלליות לניהול תיקיות משותפות והקצאת הרשאות לתיקיה משותפת:

- קבע איזה קבוצות צריכות גישה לכל משאב ואת רמת הגישה הנדרשת. תעד את הקבוצות ואת ההרשאות שלהן לכל משאב.
- הקצה הרשאות לקבוצות ולא לחשבונות משתמשים לפישוט ניהול הגישה.
- הקצה לכל משאב את ההרשאה המגבילה ביותר שעדיין מאפשרת למשתמשים לבצע את עבודתם. לדוגמה, אם משתמשים צריכים רק לקרוא מידע מתיקיה, והם לעולם לא ימחקו או יצרו קבצים, הקצה הרשאת Read.
- ארגן את המשאבים כך שתיקיות עם דרישות אבטחה זהות יהיו ממוקמות בתיקיה. לדוגמה, אם משתמשים דורשים הרשאת קריאה עבור מספר תיקיות יישומים, אחסן את תיקיות היישומים בתוך אותה תיקיה. עתה שתף תיקיה זו במקום לשתף כל תיקיית יישום בנפרד.
- השתמש בשמות שיתוף אינטואיטיביים כדי שמשתמשים יוכלו להכיר ולאתר משאבים בקלות. השתמש בשמות שיתוף השמישים בכל מערכות ההפעלה.

הערה מערכות MS-DOS, Windows 3x, **ולקוחות** **W**indows **F**or **W**orkgroups - WFW קוראים שמות שיתוף עד לפורמט 8.3. אי לכך, שמות שיתוף ארוכים יותר אינם מומלצים בסביבה מעורבת.

Windows 2000 מספקת שמות שווי-ערך לשמות בפורמט 8.3 תווים, אך השמות הנוצרים עלולים להיות לא-אינטואיטיביים למשתמשים. לדוגמה, תיקיית Windows 2000 בשם Accountants Database תופיע כ-Account~1 במחשבי לקוחות המפעילים מערכות הפעלה MS-DOS, Windows 3x, ו- Windows for Workgroups.

שיתוף תיקיות

ניתן לשתף משאבים עם אנשים נוספים על ידי שיתוף תיקיות המכילות משאבים אלה. לשיתוף תיקיה עליך להיות חבר בקבוצה מיוחסת אחת או יותר, בהתאם לתפקיד המחשב בו שוכנת התיקיה המשותפת. בעת שיתוף תיקיה תוכל לשלוט על הגישה לתיקיה על ידי הגבלת מספר המשתמשים היכולים לקבל גישה בו-זמנית. ניתן גם לשלוט על גישה לתיקיה ותכולתה על ידי הקצאת הרשאות למשתמשים נבחרים וקבוצות. ברגע שיש לך תיקיה משותפת, על המשתמשים להתחבר לתיקיה משותפת זו ונדרש שיהיה להם את ההרשאות המתאימות לקבלת גישה אליה. לאחר ששיתפת תיקיה, ייתכן שתרצה לשנותה. תוכל להפסיק את השיתוף, לשנות את שם השיתוף שלה ולשנות הרשאות משתמשים וקבוצות לקבלת גישה אליה.

דרישות לשיתוף תיקיות

במערכת Windows 2000, רק למשתמשים החברים בקבוצות המובנות Administrators, Server Operators ו-Power Users יש הרשאה לבצע שיתוף תיקיה. איזה קבוצות יכולות לשתף תיקיות על איזה מחשבים? תלוי אם המחשבים שייכים לקבוצות עבודה או domains ובסוג המחשב בו שוכנת התיקיה המשותפת:

- ב- Windows 2000 Domain, יכולים החברים בקבוצות Administrators ו-Server Operators לשתף תיקיה השוכנת בכל מחשב ב-domain. החברים בקבוצה Power Users, שהיא Loacl Group, יכולים לשתף תיקיות רק ב-Stand Alone Server או על מחשב המפעיל את מערכת ההפעלה Windows 2000 Professional בו מוגדרת הקבוצה.
- בקבוצת עבודה של Windows 2000, יכולים החברים בקבוצות Administrators, ו-Power Users לשתף תיקיות בשרת העצמאי של Windows 2000 Server או במחשב הפועל תחת מערכת הפעלה Windows 2000 Professional בו מוגדרת הקבוצה.
- משתמשים שלהם הוקצתה זכות Create Permanent Shared Objects יכולים ליצור Share (שיתוף) במחשב עבורו הוקצתה זכות זו.

הערה אם התיקיה המיועדת לשיתוף שוכנת ב-NTFS volume, למשתמשים צריכה להיות הרשאת NTFS ברמת קריאה (Read) לפחות, עבור תיקיה זו.

תיקיות ניהול משותפות

Windows 2000 משתפת תיקיות באופן אוטומטי, לצרכי ניהול. שיתופים אלה הם בעלי סיומת ($). סימן ה-$ מסתיר את התיקיה המשותפת ממשתמשים המדפדפים במחשב דרך הרשת.

השורש של כל Volume, תיקיית השורש של מערכת ההפעלה (winnt), ומיקום

מנהלי ההתקנים של ההדפסה, הן כולן תיקיות אדמיניסטרטיביות משותפות ומוסתרות הניתנות לגישה אדמיניסטרטיבית דרך הרשת.

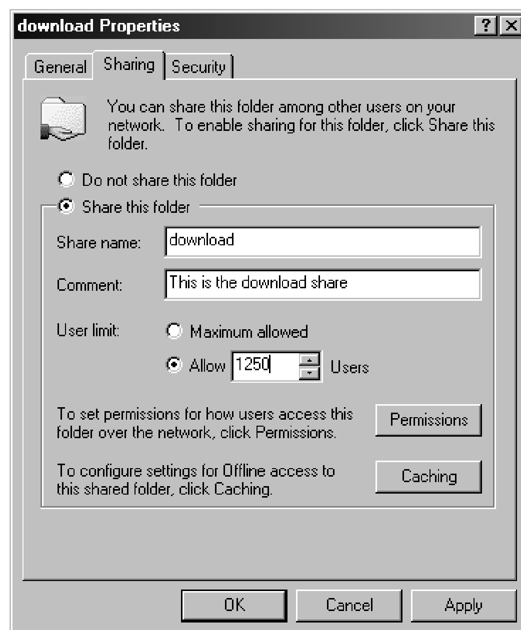
הטבלה להלן מפרטת את המטרות של תיקיות הניהול המשותפות ש-Windows 2000 יוצרת באופן אוטומטי:

שיתוף	מטרה
C$, D$, E$, וכן הלאה	השורש של כל Volume בדיסק הקשיח משותף אוטומטית, ושם השיתוף הוא אות הכונן עם סיומת $. בעת התחברות לתיקיה זו, ניתנת ל-Administrator גישה לדיסק כולו. ניתן להשתמש בשיתוף הניהולי להתחברות מרחוק למחשב לצורך ביצוע מטלות ניהוליות. Windows 2000 מקצה הרשאת Full Control (שליטה מלאה) לקבוצת Administrators. כוננים בעלי מדיה ניידת כגון כונני תקליטורים (CD) אינם מקבלים אות שיתוף מוסתרת.
Admin$	תיקיית השורש של מערכת ההפעלה, שהיא כברירת מחדל C:\Winnt, משותפת כ-Admin$. מנהלים יכולים לגשת לתיקיה משותפת זו לניהול Windows 2000 בלי לדעת באיזו תיקיה היא מותקנת. רק לחברים בקבוצת Administrators יש גישה לשיתוף זה. Windows 2000 מקצה הרשאת Full Control לקבוצת Administarators.
Print$	בעת התקנת המדפסת המשותפת הראשונה, התיקיה %systemroot%\System32\Spool\Drivers משותפת כ- Print$. תיקיה זו מספקת גישה למנהלי התקנים (Drivers) של ההדפסה עבור תחנות עבודה. רק לחברים בקבוצת Administrators, Server Operators, Print Operators יש הרשאת Full Control. לקבוצת Everyone יש הרשאת Read בלבד.

תיקיות משותפות מוסתרות אינן מוגבלות רק לאלה שהמערכת יוצרת באופן אוטומטי. ניתן לשתף תיקיות נוספות ולהוסיף את הסימן $ לסופו של שם השיתוף. רק משתמשים היודעים את שם התיקיה יכולים לגשת אליה, בתנאי שהוקצתה להם הרשאת הגישה המתאימה.

שיתוף תיקיה

בעת שיתוף תיקיה ניתן לתת לה שם שיתוף (Share Name), להוסיף הערות המתארות את התיקיה ותכולתה, להגביל את מספר המשתמשים שיש להם גישה לתיקיה, להקצות הרשאות למשתמשים שונים, ולשתף את אותה תיקיה מספר רב של פעמים. לשיתוף תיקיה, לחץ לחיצה ימנית על התיקיה אותה אתה רוצה לשתף, ולחץ Properties. מאפייני השיתוף נמצאים בכרטיסיה Sharing שבתיבת הדו-שיח של Properties (תרשים 4.10).



תרשים 4.10 הכרטיסיה Sharing בתיבת הדו-שיח Properties של התיקיה.

הטבלה הבאה מפרטת את האפשרויות בכרטיסיה Sharing:

אפשרות	תיאור
Do Not Share This Folder	עליך לבחור אפשרות זו אם אינך רוצה לשתף תיקיה. אם בחרת אפשרות זו, כל שאר האפשרויות מופיעות כבלתי פעילות.
Share This Folder	עליך לבחור אפשרות זו אם אתה רוצה לשתף תיקיה. בעת בחירת אפשרות זו, כל שאר האפשרויות פעילות.
Share Name	השם שאתו מתחברים משתמשים מאתרים מרוחקים לתיקיה המשותפת. עליך להכניס שם שיתוף (שם זה לא חייב להיות זהה לשם המקורי של התיקיה. למשל, לתיקיה קוראים Letter ושם השיתוף הוא Mooki).
Comment	תיאור אופציונלי של שם השיתוף. ההערה מופיעה כתוספת לשם השיתוף כאשר המשתמשים במחשבי לקוח מדפדפים בשרת לאיתור תיקיות משותפות, ומצב הצפייה (view) מכוון למצב פרטים (Details). ניתן להשתמש בהערה זו לצורך זיהוי תכולת תיקיה משותפת.

אפשרות	תיאור
User Limit	מספר המשתמשים המירבי שיכולים להתחבר לתיקיה משותפת בו-זמנית. אפשרות Maximum Allowed מאפשרת ל-Windows 2000 Server לתמוך במספר התחברויות בלתי מוגבל. אולם מספר **C**lient **A**ccess **L**icenses (CALs, רשיונות גישה ללקוחות) שרכשת, מגביל את ההתחברויות. ניתן גם לקבוע את מספר המשתמשים באופן ידני על ידי הכנסת מספר.
Permissions	הרשאות התיקיה המשותפת החלות רק כאשר ניגשים לתיקיה דרך הרשת. ברירת המחדל היא שקבוצת Everyone מקבלת הרשאת Full Control עבור כל התיקיות המשותפות החדשות.
Caching	הגדרות המטמון מאפשרות גישת Off-Line לתיקיה המשותפת, כך שלקוח יוכל לעבוד מול התיקיה גם אם הוא אינו מחובר On-Line לרשת (יעיל בעיקר למחשבי עגינה ומחשבים ניידים).
New Share	האפשרות ליצור שיתוף חדש, בנוסף לשיתוף הישן.
Remove Share	האפשרות להסרת שיתוף נוסף. אפשרות זו מופיעה רק לאחר שתיקיה זו שותפה יותר מפעם אחת. אין אפשרות למחוק שיתוף אדמיניסטרטיבי (כזה שנוצר אוטומטית על ידי המערכת).

לאחר ששיתפת תיקיה, השלב הבא הוא הגדרת המשתמשים שלהם תהיה גישה לתיקיה משותפת זו. הגדרה זו נעשית על ידי הקצאת הרשאות שיתוף תיקיה לחשבונות משתמשים נבחרים וקבוצות נבחרות. תוכל להקצות הרשאות על ידי לחיצה על לחצן Permission שבכרטיסיה Sharing בתיבת הדו-שיח Properties. משם, תוכל לבחור את חשבונות המשתמשים והקבוצות להם ברצונך להקצות הרשאות.

שינוי והתאמת תיקיות משותפות

ניתן לשנות ולהתאים תיקיות משותפות. לדוגמה, ניתן להפסיק את השיתוף בתיקיה, לשנות את שם השיתוף, או לשנות הרשאות של תיקיות משותפות. לשינוי והתאמת תיקיה משותפת, פתח את תיבת הדו-שיח Properties עבור תיקיה זו ובחר Sharing.

הטבלה שלהלן מפרטת את השלבים לביצוע שינויים מסוימים.

שינוי	פעולה
הפסק לשתף תיקיה	לחץ על האפשרות Do Not Share This Folder (אל תשתף תיקיה זו)
שנה את שם השיתוף	תחילה, הפסק שיתוף בתיקיה זו על ידי לחיצה על האפשרות Do Not Share This Folder. לחץ על לחצן Apply להחלת השינוי, ואז לחץ על לחצן Share This Folder (שתף תיקיה זו). הקלד את שם השיתוף החדש בתיבת הטקסט Share Name ולחץ Apply.
שנה את הרשאות השיתוף בתיקיה	לחץ על לחצן Permissions. בתיבת הדו-שיח Permissions, לחץ Add או Remove. כדי להוסיף חשבון משתמש או קבוצה, לחץ על לחצן Add ובחר בקבוצה או במשתמש בתיבת הדו-שיח Select Users, Computers or Groups המופיעה ותן את ההרשאות המתאימות.
שתף תיקיה פעמים רבות	לחץ על לחצן New Share (שיתוף חדש) כדי לשתף תיקיה בשם שיתוף נוסף. עשה זאת לצורך חיבור/צירוף כמה תיקיות משותפות לתיקיה אחת, בעודך מאפשר למשתמשים להשתמש באותו Shared Name שהשתמשו בו לפני שמיזגת את התיקיות.
הסר שם שיתוף	לחץ על לחצן Remove Share כדי להסיר שיתוף נוסף. אפשרות זו מופיעה רק לאחר שהתיקיה שותפה יותר מפעם אחת.

הערה אם אתה מפסיק שיתוף תיקיה כאשר משתמשים מחוברים אליה ויש בה קבצים פתוחים, עלולים המשמשים לאבד נתונים. אם תלחץ על לחצן Do Not Share This Folder, ומשתמש כלשהו מחובר לתיקיה זו, Windows 2000 תציג תיבת דו-שיח המודיעה לך שיש משתמש המחובר עתה לתיקיה זו.

NTFS Permissions

הרשאות NTFS הן קבוצת הרשאות סטנדרטיות המאפשרות (Allow) או מונעות (Deny) גישה לכל משתמש או קבוצה. הן מאבטחות משאבים על ידי שהן מאפשרות ל-Administarators ומשתמשים לקבוע למי תהיה גישה לקבצים ותיקיות מסוימות, ולהגדיר את סוג הגישה לכל משתמש. אבטחת NTFS יעילה בין אם ניגשים לתיקיה או קובץ במחשב מקומי (מולו יושב המשתמש) ובין אם ניגשים דרך הרשת.

Windows NT כוללת את הרשאות NTFS הסטנדרטיות הבאות :

- **NTFS Folder Permission** (הרשאת NTFS לתיקיות) – השתמש בהרשאות אלו להבטחת גישה לתיקיות מסוימות ב-NTFS formated volumes.
- **NTFS File Permission** (הרשאת NTFS לקבצים) – השתמש בהרשאות אלו להבטחת גישה לקבצים מסוימים ב-NTFS formated volumes.

הקצאת הרשאות NTFS

בעת יצירת קבצים ותיקיות חדשים, חוקים וקדימויות משפיעים על צורת ההקצאה, המיזוג והירושה של הרשאות.

הרשאת שליטה מלאה (Full Control) של NTFS

הרשאת Full Control מעניקה את כל הרשאות הגישה למשאב. היא מוקצית כברירת המחדל כדלקמן:

- ❖ כאשר משתמש יוצר קובץ או תיקיה, הוא הופך ל-Creator Owner (הבעלים והיוצר) ומוענקת לו הרשאת Full Control.
- ❖ כאשר Volume מפורמט NTFS, הרשאת Full Control מוקצית לקבוצת Everyone שבשורש הכונן.
- ❖ בעת הסבת מחיצות FAT16 או FAT32 ל-NTFS, הרשאת Full Control מוקצית לקבוצת Everyone לגבי כל המשאבים ב-Volume זה.

ריבוי הרשאות NTFS

הרשאות לקבצים ותיקיות מוקצות למשתמשים וקבוצות. ניתן להקצות למשתמשים הרשאות רבות: הרשאות המוקצות לחשבון משתמש מסוים והרשאות המוקצות לקבוצות בהן המשתמש חבר. סך ההרשאות המעשיות של משתמש הם שילוב הרשאות NTFS שהוקצו למשתמש הבודד והרשאות NTFS שהוקצו לכל הקבוצות אליהן הוא שייך. לדוגמה, אם למשתמש יש הרשאת כתיבה (Write) לתיקיה והוא גם חבר בקבוצה לה יש הרשאת קריאה (Read) לאותה תיקיה, יקבל המשתמש גם הרשאת קריאה וגם הרשאת כתיבה לתיקיה זו.

הרשאות עבור קבצי NTFS מקבלות עדיפות על הרשאות עבור תיקיות NTFS. לדוגמה, אם למשתמש יש הרשאת כתיבה לתיקיה והרשאת Modify (שינוי) לקובץ בתיקיה זו, המשתמש יכול גם לכתוב וגם לשנות קובץ זה. דבר זה נכון גם כאשר למשתמש לא הוקצתה גישה לתיקיה. משתמש תמיד יכול לגשת לקבצים שיש לו הרשאות עבורם, על ידי שימוש במוסכמות שם קובץ/שם מחשב (UNC) או נתיב לפתיחת הקובץ ביישום שלו. לדוגמה, למשתמש אין הרשאות לתיקיה המכילה קובץ שעבורו יש למשתמש הרשאת שינוי (Modify). המשתמש יכול לפתוח את הקובץ מהיישום המתאים לקובץ על ידי הקלדת שם UNC המלא, או הנתיב לקובץ זה.

מניעת הרשאה ממשתמש או קבוצה חוסמת הרשאה זו מהמשתמש, אף אם ההרשאה הוקצתה לקבוצה אליה שייך המשתמש. לדוגמה, לקבוצה Everyone הוקצתה הרשאה Full Control לקובץ אשר עבורו נמנעה ממשתמש הרשאת המחיקה (Delete). המשתמש יוכל לקרוא ולשנות את הקובץ, אך לא יוכל למחוק אותו.

הורשת הרשאות

קיימים חוקים לקדימויות של הרשאות קובץ או תיקיה ככל שתרד במורד עץ הספריה, מתיקיית ההורה לתת התיקיות ולקבצים. ברירת המחדל היא, שהרשאות הניתנות לתיקיית ההורה עוברות בירושה ומיושמות בתת התיקיות ובקבצים שבתיקיית ההורה. אבל, ניתן למנוע הורשה (Inheritance). כאשר הרשאות NTFS מוקצות או מוחלפות עבור תיקיה, ההרשאות מוקצות לתיקיה עצמה, לכל קובץ או תת תיקיה קיימים, כמו גם עבור כל קובץ או תת תיקיה חדשים שנוצרו בתיקיה. ניתן למנוע מתיקיה או קובץ לקבל בהורשה הרשאות מתיקיית ההורה, והרשאות יכולות להיות מוקצות במפורש רק לתיקיה או קובץ מסוים. כמו כן ניתן לשנות או להעביר הרשאות שהתקבלו בהורשה.

הנחיות להקצאת הרשאות NTFS

מנהלים ובעלים של קובץ או תיקיה קובעים לאיזה משתמשים וקבוצות יש הרשאות לקובץ או תיקיה, ומה סוג ההרשאות. השתמש בהנחיות הבאות בעת הקצאת הרשאות NTFS :

❖ לפישוט הניהול, קבץ משאבים לתוך תיקיות יישומים, נתונים ותיקיות בית (Home Directory). פעולה זו נותנת את היתרונות הבאים :

- הרשאות מוקצות רק לתיקיות, לא לקבצים בודדים.
- הגיבוי פשוט יותר, כיון שבדרך כלל גיבוי קבצי יישומים נמצא בעדיפות נמוכה יותר.
- כל תיקיות הבית (Home Directory) נמצאות במיקום אחד.

תיקיית הבית - תיקיה פרטית של משתמש ברשת בה נשמרים כל הנתונים של המשתמש. בדרך כלל תיקיה זו נמצאת על אחד השרתים.

❖ השתמש בהרשאות NTFS לבקרת גישה לקבצים ותיקיות. הקצה את רמת ההרשאה הנמוכה ביותר הנדרשת, למען עבודה תקינה. בכך תמנע אפשרות שמשתמשים ישנו או ימחקו מסמכים ויישומים חשובים.

❖ אם ניתן, הקצה הרשאות לקבוצות, ולא לחשבונות משתמשים בודדים. צור קבוצות בהתאם לגישה הנדרשת להם למשאבים, ואז הקצה לקבוצה כולה את ההרשאות המתאימות. הקצה הרשאות לחשבונות משתמשים בודדים רק אם נדרש.

❖ בעת הקצאת הרשאות לתיקיות הבית, רכז את תיקיות הבית ב-network volume נפרד מיישומים וממערכת ההפעלה, כדי לסייע בגיבוי נתונים וניהול.

❖ בעת הקצאת הרשאות לנתונים פעילים או תיקיות יישומים, הסר את הרשאת Full Control של ברירת המחדל מקבוצת Everyone. הקצה הרשאות קריאה (Read) וביצוע (Execute) לקבוצות המשתמשים והמנהלים. בכך ימנעו מחיקה

בשוגג של קבצי יישומים או פגיעה בהם על ידי משתמשים או וירוסים. ניתן להעניק ל-Administrators ולמשתמשים, האחראים לשדרוג יישומי איתור תקלות, הרשאת Full Control, ולאחר סיום משימתם להחזירם להרשאת קריאה וביצוע.

- בעת הקצאת הרשאות לתיקיות נתונים ציבוריות, הקצה הרשאות Add (הוספה), Read (קריאה) ו- Execute (ביצוע) לקבוצת המשתמשים, והרשאת Full Control ליוצר והבעלים של התיקיה. כך ניתנת למשתמשים יכולת למחוק ולשנות רק את הקבצים והתיקיות שהם יצרו, בנוסף ליכולת קריאת מסמכים שנוצרו על ידי אחרים.
- ככלל, עדיף שלא להקצות הרשאות, מאשר למנוע הרשאות. מנע (Deny) הרשאות רק כאשר יש צורך חיוני למנוע גישה ייחודית לחשבון משתמש או קבוצה ייחודית.
- עודד וחנך את המשתמשים להקצות הרשאות לקבצים ותיקיות שהם יוצרים והם בבעלותם. ספק להם הנחיות להקצאת NTFS הרשאות מתאימות למשאבים שבשליטתם.

הגדרת הרשאות NTFS

בעלי קבצים ותיקיות יכולים להקצות הרשאות לחשבונות משתמשים ולקבוצות. גם מנהלים יכולים להקצות הרשאות למשאבים אלה.

כדי להקצות או לשנות הרשאות NTFS לקובץ או תיקיה, פתח את תיבת הדו-שיח Properties עבור קובץ או תיקיה זו. הרשאות NTFS מוגדרות בכרטיסיה Security של תיבת הדו-שיח Properties. בטבלה להלן מפורטות האפשרויות בכרטיסיה Security.

אפשרות	תיאור
Name	רשימת חשבונות משתמשים או קבוצות עם הרשאות לקובץ או תיקיה. לחץ על לחצן User Account או Group להקצאה או שינוי הרשאות, או הסרה מהרשימה.
Permissions	ההרשאות שניתן לאפשר לחשבון המשתמש או קבוצה, או למנוע: בחר בתיבת הסימון Allow לאפשר הרשאה. בחר בתיבת הסימון Deny למניעת הרשאה.
Add	לחץ על לחצן זה לפתיחת תיבת הדו-שיח Select Users, Groups, or Computers בה תוכל לבחור חשבונות משתמשים וקבוצות, שלהן יש הרשאות לאובייקט, ולהוסיפן לרשימת השמות.

אפשרות	תיאור
Remove	לחץ על לחצן זה להסרת חשבון משתמש או קבוצה שנבחרו בעבר ואת ההרשאות המשויכות מהקובץ או התיקיה.
Allow Inheritable Permissions From Parent To Propagate To This Object	אפשרות זו מסומנת, כברירת מחדל, בכל האובייקטים והמשמעות היא שמתקיימת ירושת היררכיה, כך שכל התת-תיקיות והקבצים מקבלים את ההרשאות שהוקצו לתיקיית ההורה באופן אוטומטי. הרשאות שנרכשו מתיקיית הורה מסומנות עם רקע אפור ולא ניתן לבטל אותן, אך ניתן להוסיף הרשאות או מניעות נוספות. כדי לבטל או לשנות הרשאות/מניעות נרכשות, יש לבטל קודם את אפשרות זו.
Advanced	לחץ על לחצן זה לפתיחת תיבת הדו-שיח Access Control Settings. כאן ניתן להגדיר הרשאות גישה מיוחדות, יכולת ביצוע מעקב (Audit) ובקרת בעלות (Creater Owner) על קבצים ותיקיות.

הקצאת הרשאות גישה מיוחדות

ככלל, הרשאות NTFS הסטנדרטיות מספקות את כל ההרשאות הנדרשות לאבטחת מידע. אולם, יש מקרים בהם ההרשאות הסטנדרטיות אינן מאפשרות את הגישה המיוחדת הנדרשת. ליצירת גישה מיוחדת, השתמש בהרשאות NTFS מיוחדות. כמו בהרשאות רגילות, הרשאות גישה מיוחדות ניתנות או נמנעות.

הערה בעת הקצאת הרשאות גישה מיוחדות לקבוצת משתמשים, ההרשאות מצוינות כ-Special (מיוחדות) בתיבת הדו-שיח של Access Control Settings.

הרשאות גישה מיוחדות מספקות שליטה מדויקת יותר להקצאת גישה למשאבים. קיימות 13 הרשאות גישה מיוחדות, ששילובן יוצר את הרשאות NTFS הסטנדרטיות, כגון Read & Execute (קריאה וביצוע), Modify (שינוי), ו- Full Control (שליטה מלאה). לדוגמה, הרשאת הקריאה הסטנדרטית של NTFS כוללת את הרשאות Read data (קריאת נתונים), Read attributes (קריאת מאפיינים) ו- Read extended attributes (קריאת מאפיינים מורחבים).

הקצאת הרשאות גישה מיוחדות לתיקיות וקבצים דורשת שלוש מטלות:

- ❖ הגדרת הרשאות ממוקדות יותר
- ❖ העברת בעלות
- ❖ בחינת גישה

שינוי הרשאות

בעלי תיקיות (Creater Owner), קבצים ומשתמשים אחרים בעלי הרשאות Full Control יכולים להקצות או להחליף הרשאות. ניתן להעניק למנהלי הרשת את היכולת לשנות הרשאות בקובץ או תיקיה, מבלי לתת להם Full Control על התיקיה או הקובץ. בדרך זו, המנהל יכול להקצות הרשאות אך לא תהיה לו הרשאה למחוק קובץ או תיקיה, או לכתוב אליהם. כדי לתת למנהלי רשת את היכולת לשנות הרשאות, הענק לקבוצת מנהלי הרשת את ההרשאה המיוחדת עבור התיקיה או הקובץ ב-Change Permissions.

אם חבר בקבוצת Administartors לוקח בעלות, אז כל קבוצת Administartors הופכת לבעלים, וכל חבר בה יכול לגשת ולשנות את ההרשאות עבור התיקיה או הקובץ.

העברת בעלות

בנוסף להעברת הרשאות, ניתן גם להעביר בעלות. ישנן מספר דרכים להעביר בעלות:

- הבעלים הנוכחיים יכול להקצות את הרשאת Full Control הסטנדרטית או את הרשאת הגישה המיוחדת Take Ownership (לקיחת בעלות) למשתמשים אחרים, ובכך לאפשר למשתמשים אלה לקחת בעלות.
- Administrator יכול לקחת בעלות על כל קובץ או תיקיה שתחת ניהולו. לדוגמה, אם עובד עזב את החברה, Administrator יכול לקחת בעלות על הקובץ של אותו עובד ולשנות את ההרשאות, כך שאחרים יוכלו לגשת לקבצים או לתיקיות.
- בעת הקצאה לתיקיה או קובץ, הרשאות גישה מיוחדות מוחלות תחילה רק במקומות שהוגדרו בתפריט הנפתח Apply Onto, הנידון ביתר פירוט בהמשך שיעור זה.

להעברה או לקיחת בעלות על קובץ או תיקיה, בחר בכרטיסיה Owner בתיבת הדו-שיח Access Control. הבעלים הנוכחיים של הקובץ או התיקיה מוצג בתיבת הטקסט Current Owner Of This Item. ניתן לבחור בעלים חדשים מהרשימה Change Owner To. ניתן גם לבחור בתיבת סימון Replace Owner Or Subdirectories And Objects לשינוי הבעלות של כל תת התיקיות והקבצים הכלולים בתיקיה.

הגדרת הרשאות גישה מיוחדות

להגדרת הרשאות גישה מיוחדות, גש לתיבת הדו-שיח Properties של קובץ או תיקיה, ולחץ Advanced בכרטיסיה Security. בתיבת הדו-שיח Access Control Settings, לחץ על הכרטיסיה Permissions, ולחץ Add להוספת משתמש חדש או קבוצה, ולשינוי הרשאות הגישה המיוחדות. לחץ View/Edit לשינוי זכויות הגישה המיוחדות של משתמש או קבוצה קיימים. מכאן תוכל להגדיר את האפשרויות להגדרת הרשאות גישה מיוחדות. אפשרויות אלה מפורטות בטבלה להלן.

אפשרות	תיאור
Name	שם חשבון המשתמש או הקבוצה. לבחירת חשבון משתמש או קבוצה שונים, לחץ על לחצן Change.
Apply Onto	רמת היררכיית התיקיה בה עוברות הרשאות NTFS המיוחדות בירושה. ברירת המחדל היא This Folder, Subfolders, Files.
Permissions	הרשאות גישה בודדות מיוחדות. להקצאת או למניעת הרשאת גישה מיוחדת בודדת של NTFS, בחר בתיבת סימון Allow או Deny בהתאמה.
Apply These Permissions To Objects And/Or Containers Within This Container Only	תיבת סימון זו זמינה לתיקיות ותת תיקיות. תיקיות נמוכות יותר בהיררכיית התיקיות יכולות לרשת הרשאות NTFS בודדות מעודכנות מתיקיה זו. אפשרות זו אינה זמינה עבור קבצים. לחץ להסרת סימון מתיבה זו למניעת הורשת הרשאות. בחר בתיבת סימון זו ליצור ריבוי הרשאות NTFS בודדות מעודכנות במורד היררכיית התיקיות .
Reset Permissions On All Child Objects And Enable Propagation Of Inheritable Permissions	תיבת סימון זו זמינה רק עבור מחיצות. ממחיצה, ניתן לאפס הרשאות עבור כל התיקיות, תת התיקיות והקבצים. בחר בתיבת סימון זו כדי שכל ההרשאות עבור קבצים או תיקיות שבמחיצה זו יאופסו להגדרות שהוקצו למחיצה כולה. אפשרות זו גם כוללת את תיבת הסימון Apply These Permissions To Objects And/Or Containers Within This Container Only (החל הרשאות אלה על אובייקטים ו/או מכולות במכולה זו בלבד). תיבת דו-שיח זו מוסברת בשורה הקודמת.
Clear All	מחק את כל ההרשאות שנבחרו ואת רמת ההיררכיה של התיקיות שנבחרו לרשת הרשאות.

הטבלה הבאה סוקרת את האפשרויות הזמינות בתפריט הנפתח Apply Onto (החל על):

אפשרות	אובייקטים שעליהם חלה האפשרות
This Folder Only	תיקיה זו בלבד.
This Folder, Subfolders, And Files	תיקיה זו, תת תיקיות ולקבצים כולם.
This Folder And Subfolders	תיקיה זו ותת תיקיות אך לא על קבצים.
This Folder And Files	תיקיה זו ולקבצים שלה בלבד.
Subfolders and Files Only	תת תיקיות ולקבצים בלבד, אך לא תחול על תיקיה נוכחית (כן תחול על קבצים בתיקיה נוכחית).
Subfolders Only	תת תיקיות בלבד. האפשרות אינה חלה על תיקיה נוכחית וגם לא על קבצים.
Files Only	קבצים בלבד. האפשרות אינה חלה על התיקיה הנוכחית וגם לא על תת תיקיות.

הערה כל קובץ או תת תיקיה שיווצרו, לאחר מכן ירשו כברירת מחדל את הרשאות התיקיה.

העתקה והעברת קבצים ותיקיות

NTFS מאפשרת העתקה והעברת קבצים ותיקיות.

העתקת קבצים ותיקיות

להעתקת קבצים ותיקיות בין או בתוך NTFS Volumes, יש להעניק למשתמש הרשאת Create Files/Write Data ו-Creat Folder/Append Data עבור תיקיית היעד. המשתמש שמבצע את ההעתקה הופך לבעליו (Creater Owner) של הקובץ או התיקיה.

בעת העתקת קבצים או תיקיות, הרשאות יעברו בירושה או יאבדו, בהתאם ליעד ההעתקה של הקובץ או התיקיה:

- כאשר קובץ או תיקיה מועתקים בתוך או בין מחיצות NTFS, הקובץ או התיקיה יורשים את ההרשאות של תיקיית היעד.

❖ כאשר קובץ או תיקיה מועתקים ל-FAT16 volumes או ל-FAT32 volumes, הקבצים או התיקיות מאבדים את הרשאות NTFS שלהם, כיון ש-FAT16 volumes ו-FAT32 volumes אינם תומכים בהרשאות NTFS.

העברת קבצים ותיקיות

העברת קבצים ותיקיות בין מחיצות NTFS מחייב הרשאת Add לקובץ או תיקיית היעד, והרשאת Delete עבור קובץ או תיקיית המקור. הרשאת Delete נדרשת להעברת קובץ או תיקיה, כיון שלאחר שהועברו לתיקיית היעד הקובץ או התיקיה נמחקים מתיקיית המקור. כאשר מזיזים תיקיה או קובץ למחיצה אחרת, המשתמש שביצע את ההעברה יהפוך ל-Creator Owner (בעלים יוצר).

העברת תיקיות וקבצים בתוך ובין NTFS volumes עשויה להשפיע על ההרשאות המקוריות. הטבלה שלהלן מפרטת את התוצאות של תרחישי העברת קובץ או תיקיה.

פעולה	תוצאה
העברת קבצים ותיקיות בתוך אותו Volume (Intra-volume)	הקובץ או התיקיה שומרים על הרשאותיהם המקוריות.
העברת קבצים ותיקיות בין Volumes (Inter-volume)	הקובץ או התיקיה יורשים את ההרשאות שהוגדרו בתיקיית היעד.

כאשר קבצים ותיקיות מועברים ל-FAT16 volumes או ל-FAT32 volumes, הקבצים והתיקיות מאבדים את הרשאות ה-NTFS שלהם, כיון ש-FAT16 volumes ו-FAT32 volumes אינן תומכות בהרשאות NTFS.

הערה לאחר שתלמד כיצד ליצור משתמשים וקבוצות בפרקים מאוחרים יותר, תחיל הרשאות שיתוף והרשאות NTFS למשתמשים ולקבוצות שיצרת.

איתור תקלות בהרשאות NTFS

הטבלה הבאה מתארת תקלות הרשאה נפוצות ומספקת פתרונות :

תקלה	פתרון
משתמש אינו מקבל גישה לקובץ או לתיקיה.	בדוק את ההרשאות שהוקצו לחשבון המשתמש ולקבוצות בהן המשתמש חבר. אם נמנעה גישה לקובץ או לתיקיה ממשתמש או מקבוצה אליה הוא שייך, למשתמש לא תהיה גישה למשאב. אם הקובץ או התיקיה הועתקו בתוך מחיצת NTFS, או הועתקו או הועברו למחצית NTFS אחרת, ייתכן שההרשאות השתנו, עקב הורשת הרשאות חדשות מתיקיית היעד. אם הוגדרו זכויות שיתוף וגם הרשאות NTFS בתיקיה, יחולו ההרשאות המגבילות יותר.

תקלה	פתרון
חשבון משתמש מתוסף לקבוצה כדי להקצות למשתמש מסוים גישה לקובץ או תיקיה, אך המשתמש עדיין אינו יכול לגשת לקובץ או לתיקיה.	אסימון גישה (Access Token) נוצר בכל פעם שמשתמש מתחבר (Logon), והוא מאומת על ידי מחשב המפעיל Windows NT או Windows 2000. אסימון הגישה מכיל נתונים אודות הקבוצות אליהם שייך המשתמש. כדי לעדכן את אסימון הגישה כך שיכלול גם את הקבוצה החדשה, על המשתמש להתנתק (Logoff) ולהתחבר (Logon) שנית.
משתמש מוחק קובץ, אף שלמשתמש זה אין הרשאה למחוק קובץ.	הקצה את כל ההרשאות ברמת התיקיה, ולא ברמת הקובץ. למניעת גישה ממשתמשים מסוימים, קבץ קבצים בתיקיה נפרדת ואז הקצה לתיקיה זו גישה מוגבלת. אם בעיה זו בלתי ניתנת למניעה, על תקצה הרשאת Full Control לתיקיה. במקום זאת, הקצה את כל ההרשאות, כלומר, הרשאות מסוג: Modify (שינוי), Read & Execute (קריאה וביצוע), List Folder Contents (הצגת רשימת תכולת תיקיה), Read (קריאה) ו- Write (כתיבה). כך ניתנות כל היכולות של הרשאת Full Control עבור התיקיה ותכולתה, פרט לכך שמשתמשים אינם יכולים למחוק קבצים בתוך התיקיה (בעיה זו קיימת רק במערכות התומכות בתת-מערכת Posix).

סיכום שיעור

ניתן לשתף תיקיות כך שמשתמשים יוכלו להתחבר לתיקיה דרך הרשת ולקבל גישה לקבצים שבתוכה. אולם, לקבלת גישה לקבצים, נדרש שלמשתמשים יהיו הרשאות גישה לתיקיות המשותפות. הרשאות תיקיה משותפת חלות על התיקיה ולא על קבצים בודדים. כאשר יוצרים שיתוף בתיקיה ניתן לתת לה שם שיתוף, להוסיף הערות לתיאור התיקיה ותכולתה, להגביל את מספר המשתמשים להם יש גישה לתיקיה, להקצות הרשאות וליצור מספר שיתופים לאותה תיקיה. הרשאות תיקיה משותפת הן הדרך היחידה לאבטחת משאבי הרשת ב-FAT volumes. הרשאות NTFS אינן זמינות במחיצות FAT. הרשאות NTFS הן קבוצת הרשאות סטנדרטיות המאפשרות או מונעות גישה ממשתמשים או מקבוצות. ברירת המחדל היא שהרשאות המוקצות למחיצה ותיקיית ההורה עוברות בירושה, ואינן מיושמות על תת התיקיות והקבצים בתיקיית ההורה. הבעלים של קובץ או תיקיה והמנהל קובעים לאיזה משתמש וקבוצה יהיו הרשאות לתיקיה או קובץ, ומה מהות ההרשאות. בעלים של קבצים ותיקיות יכולים להקצות הרשאות לחשבונות משתמשים ולקבוצות. גם מנהלים יכולים להקצות הרשאות למשאבים אלה.

שאלות סיכום

השאלות הבאות נועדו לחזק את שליטתך בנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות לשאלה, עיין בשיעור המתאים ונסה לענות על השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואח״כ בעברית.

The following questions are intended to reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A.

1. You install a new 10- GB disk drive that you want to divide into five equal 2- GB sections. What are your options?
2. You are trying to create a striped volume on your Windows 2000 Server to improve performance. You confirm that you have enough unallocated disk space on two disks in your computer, but when you right- click an area of unallocated space on a disk, your only option is to create a partition. What is the problem, and how would you resolve it?
3. You dual boot your computer with Windows 98 and Windows 2000. You upgrade Disk 1, which you are using to archive files, from basic storage to dynamic storage. The next time you try to access your files on Disk 1 from Windows 98, you are unable to read the files. Why?
4. What is the default permission when a partition is formatted with NTFS? Who has access to the volume?
5. If a user has Write permission for a folder and is also a member of a group with Read permission for the folder, what are the user 's effective permissions for the folder?
6. What happens to permissions that are assigned to a file when the file is moved from one folder to another folder on the same NTFS partition? What happens when the file is moved to a folder on another NTFS partition?
7. If an employee leaves the company, what must you do to transfer ownership of his or her files and folders to another employee?
8. What is the best way to secure files and folders that you share on NTFS partitions?

1. התקנת דיסק 10GB חדש ואתה רוצה לחלק אותו לחמישה קטעים בני 2GB כל אחד. מה האפשרויות העומדות בפניך?

2. אתה מנסה ליצור Striped Volume בשרת Windows 2000 Server שלך, לשיפור ביצועים. אתה מוודא שיש לך די שטח בלתי מוקצה בשני דיסקים במחשב שלך, אך כאשר אתה לוחץ לחיצה ימנית על שטח בלתי מוקצה בדיסק, האפשרות היחידה המוצגת היא יצירת מחיצה (partition). מה הבעיה וכיצד תפתור אותה?

3. אתה מבצע אתחול כפול במחשב שלך, עם Windows 98 ו-Windows 2000. אתה משדרג את דיסק 1, המשמש לאחסון קבצי ארכיב, מתצורת אחסון בסיסי לאחסון דינמי. בפעם הבאה שתנסה לגשת לקבצים שלך בדיסק 1 מ-Windows 98, אינך יכול לקרוא קבצים אלה. מדוע?

4. מהן הרשאות ברירת המחדל כאשר מחיצה מפורמטת עם NTFS? למי יש גישה ל-Volume?

5. אם למשתמש יש הרשאת כתיבה לתיקיה, והוא גם חבר בקבוצה עם הרשאת קריאה לתיקיה זו, מה הן ההרשאות המעשיות של משתמש זה בתיקיה זו?

6. מה קורה להרשאות המוקצות לקובץ כאשר הוא מועבר מתיקיה אחת לשנייה באותה מחיצת NTFS? מה קורה כאשר הקובץ מועבר לתיקיה הנמצאת על מחיצת NTFS אחרת?

7. אם עובד עזב את החברה, מה עליך לעשות להעברת הבעלות על הקבצים או התיקיות שלו לעובד אחר?

8. מהי הדרך הטובה ביותר לאבטח קבצים ותיקיות משותפים במחיצות NTFS?

פרק 5

מערכות קבצים מתקדמות

אודות פרק זה

פרק זה מציג בפניך את הנושאים **מערכת קבצים מבוזרת** (**D**istributed **F**ile - Dfs) **S**ystem) **ושירות שכפול קבצים** (**F**ile **R**eplication **S**ervice - FRS). Dfs מאפשרת למנהלי מערכות להקל על גישה וניהול של משתמשים המבוזרים פיסית על פני הרשת. באמצעות Dfs קבצים המפוזרים על פני מספר רב של שרתים ייראו למשתמשים כאילו הם שוכנים בנקודה אחת ברשת. משתמשים אינם צריכים לדעת ולציין את המיקום הפיסי האמיתי של קבצים כדי לגשת אליהם.

Dfs משתמשת ב-FRS לסינכרון אוטומטי של תוכן בין עותקים משוייכים. תוסף התוכנה Microsoft Active Directory Sites And Services משתמש ב-FRS לשכפול הטופולוגיה וקטלוג הנתונים הגלובלי (Global Catalog) על פני בקרי תחומים (Domain Controlers).

לפני שתתחיל

לביצוע השיעורים בפרק זה נדרש:

❖ השלמת כל התרגילים הקודמים כך ששני המחשבים פועלים תחת מערכות הפעלה Windows 2000 Server ומוגדרים כמפורט בתרגילים.

שיעור 1:
Dfs - Distributed File Systems

Dfs (Distributed File System) עבור Windows 2000 Server מספקת למשתמשים גישה נוחה לתיקיות משותפות המפוזרות ברשת כולה. תיקיית Dfs משותפת אחת משמשת כנקודת גישה מרכזית לתיקיות משותפות אחרות ברשת.

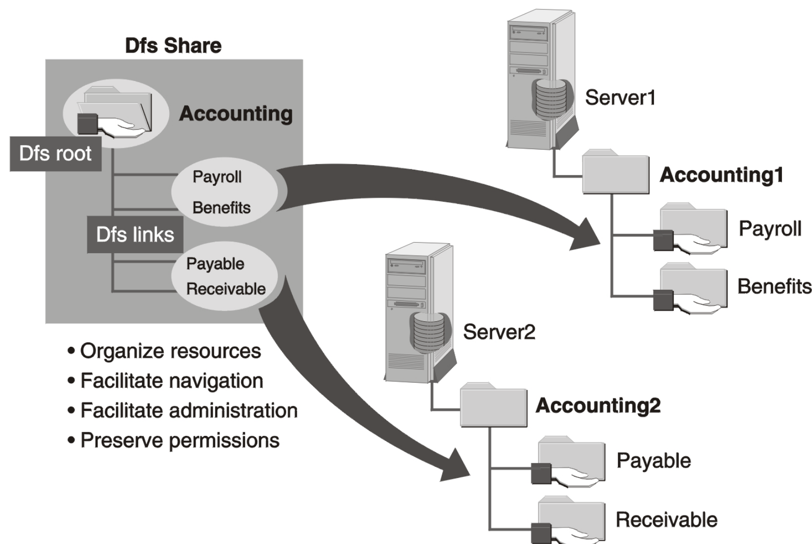
לאחר שיעור זה, תוכל

- להגדיר Stand-Alone Dfs Root.
- להגדיר קישור Dfs Link.
- להגדיר Domain Dfs Root.

זמן לימוד משוער: 35 דקות

מבוא ל-Dfs

Dfs היא מערכת קבצים היררכית לוגית בודדת. היא מארגנת תיקיות משותפות במחשבים שונים ברשת כדי ליצור מבנה עץ לוגי עבור משאבי מערכות קבצים. תרשים 5.1 מתאר כיצד Dfs יכולה לארגן משאבים השוכנים ברכיבים שונים של הרשת.



תרשים 5.1 דוגמה של שיתוף Dfs.

כיון שעץ Dfs הוא נקודת התייחסות בודדת, ללא תלות במיקומם האמיתי של המשאבים שהוא מייצג, ניתנת למשתמשים גישה קלה למשאבי הרשת. כמתואר בתרשים 5.1, משאבי הקבצים של הנהלת חשבונות במספר שרתים רב, מאורגנים בשורש Dfs לוגי אחד בשם Accounting.

משתמש המנווט בתיקיה משותפת המנוהלת על ידי מערכת Dfs, אינו צריך לדעת את שם השרת עליו נמצאת התיקיה המשותפת. דבר זה מפשט את הגישה לרשת, כיון שמשתמשים אינם צריכים עוד לאתר את השרת בו שוכנים משאבים נדרשים. לאחר התחברות לשורש Dfs, המשתמשים יכולים לדפדף ולקבל גישה לכל המשאבים שמתחת לשורש זה, ללא תלות במיקום השרת בו הם שוכנים. בדוגמה מעלה, משתמשים הרוצים גישה לקבצי הנהלת חשבונות יוכלו לאתר אותם בנקודה אחת זו.

שיתוף Dfs הוא מבנה עץ המכיל שורש וקישורי Dfs. ליצירת שיתוף Dfs, עליך ליצור תחילה שורש Dfs (Dfs Root). לכל שורש Dfs יכולים להיות קישורי Dfs (Dfs Links) רבים, אשר כל אחד מהם מצביע לעבר תיקיה משותפת ברשת. קישורי Dfs של שורש Dfs מייצגים תיקיות משותפות (<computer_name>\<share_name>) העשויות לשכון פיסית בשרתי מחשבים שונים.

הטבלה להלן מפרטת את יתרונות Dfs :

פעולה	יתרונות
ניהול רשת	Dfs מפשטת את ניהול הרשת. אם שרת אינו תקין, ניתן להעביר קישור Dfs משרת אחד לשני, מבלי שהמשתמשים יבחינו בשינוי. כל שנדרש כדי להעביר קישור Dfs הוא לשנות את הייחוס של תיקיית Dfs כך שתתייחס למיקום החדש של הקבצים המשותפים בשרת החדש. המשתמשים ממשיכים להשתמש באותו נתיב Dfs עבור קישור ה-Dfs.
טווח שמות	לקוחות ניגשים למשאבי קבצים על ידי שימוש בטווח שמות יחיד (שורש Dfs), בניגוד למיפוי אותיות כוננים לוגיים ברחבי הארגון כולו.
צריכת זיכרון	לקוחות Windows 2000 ולקוחות Windows NT אינם צורכים זיכרון נוסף, כיון שתמיכת Dfs מובנית לתוך מנתב (Redirect) לקוח Microsoft גם ב-Windows 2000 וגם ב-Windows NT. יש להתקין את Dfs Service For Microsoft Network Client מעל מנתב לקוחות Microsoft מבוססי Windows 9x, כדי שלקוח מבוסס Windows 32 סיביות יוכל לגשת לשיתוף Dfs. אם לא הותקן שירות זה, לקוחות Windows 9x יכולים לגשת לשיתופים סטנדרטיים בלבד.

פעולה	יתרונות
החלפת שרתים	Administrators יכולים להחליף שרתי קבצים, מבלי להשפיע על טווח השמות שמשמש את לקוחות הרשת, פשוט על ידי עדכון הנתיב לשרת החדש באמצעות תוסף התוכנה Distributed File System (מערכת קבצים מבוזרים).
איזון עומסים ו-Fault tolerance	Dfs מספקת מידה של איזון עומסים (Load Balancing) וסיבולת תקלות (Fault Tolerance), כיון שלקוחות בוחרים להתחבר לשרת פיסי בצורה אקראית, מתוך רשימת החלופות שמציג שרת Dfs.
יכולת התרחבות	טווח השמות של Dfs ניתן להרחבה בכל עת, כדי לשלב שטח דיסק נוסף או דרישות עסקיות חדשות.
הרשאות רשת	Dfs שומרת על הרשאות רשת. לא נדרשות כל הרשאות חדשות או תוספת אבטחה, כיון ש-Dfs volumes משתמשים בהרשאות קבצים ובתיקיות הקיימות של Windows 2000. ACL על שכפולי Windows 2000 בעלי Fault tolerance, גם כן משוכפלים.
מטמון לקוחות	לקוחות Dfs מכניסים משאבי רשת שהשימוש בהם רב, למטמון, ובכך מונעים עיכובים באיתור שרתים. הגישה הראשונה לעץ Dfs תלווה בירידה קלה בביצועים (שווה ערך לביצוע פקודת Net Use). הכנסת נתונים אלה למטמון מונעת ירידה בביצועים בגישות הבאות, עד שהלקוח מבצע אתחול (Reboot) מחדש או שהמטמון מאבד תוקף.
הטמעת Internet Information (IIS) Services	Dfs פועל עם IIS. אם הדף הראשון מועבר פיסית משרת אחד לשרת אחר לא נדרש לעדכן קישורים לדפים אחרים המאוחסנים ב-Dfs. זאת, בתנאי שה-Administrator יגדיר מחדש את ה-Dfs בהתאם. אם השרת המארח דף אינטרנט נותק מהרשת, והדף מוצג מחדש במקום אחר כלשהו, לא יהיה צורך לחזור ולהגדיר את הקישורים בדף זה.

מגבלות Dfs

הטבלה להלן מפרטת את מגבלות Dfs:

תיאור	מגבלה
מספר תווים מירבי לכל נתיב קובץ	260
מספר החלפות מירבי לכל volume	32
מספר שורשי Dfs לכל שרת	1

תיאור	מגבלה
מספר שורשי Dfs לכל Domain	לא מוגבל
מספר מירבי של volumes המתארחים ב-Domain או enterprise	מוגבל על ידי משאבי המערכת. 6,000 נבדקו בהצלחה ב-Stand-Alone roots.

הערה מסמך "Distributed File System: A logical View Of Physical Storage" ("מערכת קבצים מבוזרת: נקודת מבט לוגית של אחסון פיסי") כולל פרטים אודות חליפות ונקודות אחרות המתייחסות ל-Dfs.

עיין בתקליטור המצורף לספר זה בתיקיה \chapt05\articles\compaq.html.

סוגים של שורשי Dfs

שירות Dfs מותקן אוטומטית בעת התקנת Windows 2000 Server. השירות ניתן להשהיה, הפסקה והתחלה, אך לא ניתן להסירו ממערכת ההפעלה.

ניתן להגדיר שני סוגי שורשים ב-Windows 2000 Server:

1. שורשי Dfs עצמאיים (Stand-Alone),
2. שורשי תחומים (Domain) של Dfs (הנקראים לעיתים גם שורשי Dfs בעלי Fault tolerance).

Stand-Alone Dfs Root

שורשי Dfs עצמאיים (Stand-Alone Dfs Root) כוללים את האפיונים הבאים:

- ❖ נתוני Dfs עצמאיים מאוחסנים באוגר המקומי של שרת Stand-Alone (שרת עצמאי שאינו שייך ל-Domain).
- ❖ Dfs עצמאי מאפשר קישורי Dfs ברמה אחת בלבד.
- ❖ בעת שימוש בתוסף תוכנה Distributed File System כדי להתחבר לשורשי Dfs קיימים, כל השרתים הידועים לרשימת הדפדוף מאוחזרים, כיון שלא קיים שם NetBios ייחודי שנרשם על ידי שרתים עם Dfs מופעל.
- ❖ ניתן להתקין שורשי Dfs עצמאיים בכל מערכות הקבצים הנתמכות, אף שמומלץ להתקין משאבים במחיצות מפורמטות NTFS.
- ❖ שורשי Dfs עצמאיים אינם מאפשרים שכפול או גיבוי; כתוצאה מכך, שורש Dfs מהווה נקודת כשל יחידה (החוליה החלשה במערכת). ניתן ליצור העתק משורש Dfs עצמאי; אולם שירותי שכפול קבצים אינם זמינים בשרת Stand-Alone.

Domain Dfs Root

שורשי Dfs עם Fault tolerance (המכונים גם שורשי Dfs של domains, Domain Dfs Root), כוללים את האפיונים הבאים:

- בשורש Dfs של domain, שרתים רבים מנפיקים הפניות לטווח השמות של Dfs. שורשי Dfs בעלי Fault tolerance משתמשים בשירותי Active Directory לשמירת טופולוגיית עצי Dfs ולהסרת השורש כנקודת כשל יחידה.
- שורש Dfs בעל Fault tolerance מאוחסן בשירותי Active Directory ומשוכפל בכל שורש Dfs בכל שרת משתתף. שינויים בעץ Dfs מתואמים אוטומטית עם שירותי Active Directory. כך מובטח שתמיד תוכל לשחזר טופולוגיית עץ Dfs אם שורש Dfs אינו מקוון מסיבה כלשהי. תוכל גם להחיל Fault tolerance ברמת הקובץ או התוכן, על ידי הקצאת משאבים חליפיים ל-Dfs volume. ניתן לשרת כל צומת ענף בעץ Dfs באמצעות ערכת משאבים משוכפלים. אם חיבור לקוח למשאב חליפי נכשל מסיבה כלשהי, לקוח Dfs ינסה להתחבר לאחר. לקוח Dfs עובר בין החליפות בצורה מחזורית עד שהוא מאתר חלופה זמינה.
- שורשים עם Fault tolerance חייבים להיות מותקנים על מחיצות מפורמטות NTFS 5.0.
- רשימת התחומים והשרתים מתאכלסת על ידי ביצוע שאילתות בקטלוג הגלובלי (Global Catalog) עבור כל שורשי Dfs בעלי Fault tolerance (ObjectClass=ftDfs).
- טופולוגיית השכפול של Dfs מסתמכת על טופולוגיית שכפול Active Directory הקיימת ואין צורך במערכת שכפול Dfs נוספת.

הגדרת Dfs

Windows 2000 מאפשרת הגדרת שורשי Dfs עצמאיים, קישורי Dfs ושורשי תחומים של Dfs.

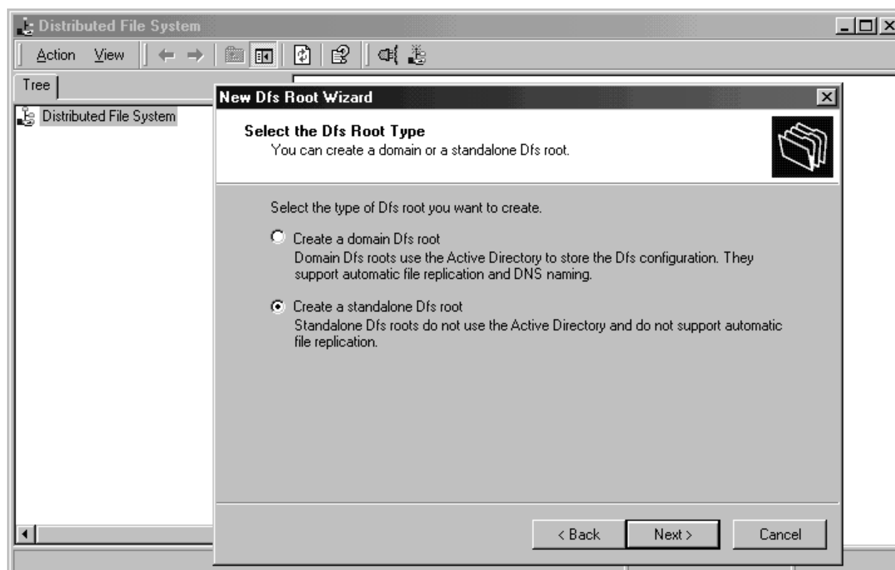
הגדרת Stand-Alone Dfs Root

Dfs עצמאיים מאחסנים את טופולוגיית Dfs במחשב אחד בודד. Dfs מסוג זה אינו מספק Fault tolerance כלל.

שורש Dfs עצמאי ממוקם פיסית בשרת שאליו מתחברים המשתמשים לראשונה. השלב הראשון להגדרת Dfs עצמאיים היא יצירת שורש Dfs.

ליצירת Stand-Alone Dfs Root (שורש Dfs עצמאי), השתמש בתוסף התוכנה Distributed File System להתחלת אשף New Dfs Root.

תרשים 5.2 מתאר את מסך Select the Dfs Root Type כאשר לחצן אפשרויות Create A Standalone Dfs Root, נבחר כברירת מחדל.



תרשים 5.2 יצירת Stand-Alone Dfs Root באמצעות תוסף התוכנה Distributed File System.

הטבלה להלן מפרטת את המסכים באשף ואת הפעולות שתוכל לבצע להגדרת שורש Dfs החדש:

מסך	פעולה
Select The Dfs Root Type (בחר סוג שורש Dfs)	בחר באפשרות Create A Stand Alone Dfs Root (צור שורש Dfs עצמאי) כמוצג בתרשים 5.2.
Specify The Host Server For The Dfs Root (הגדר את השרת המארח עבור שורש Dfs)	הקלד את נקודת החיבור הראשונה עבור כל המשאבים שבעץ Dfs. תוכל ליצור שורש Dfs על כל מחשב המפעיל Windows 2000 Server.
Specify The Dfs Share (הגדר את שיתוף Dfs)	הקלד שם תיקיה משותפת לאירוח שורש Dfs. ניתן להשתמש בתיקיה משותפת קיימת, או ליצור חדשה.
Name The Dfs Root (תן שם לשורש Dfs)	הקלד שם המתאר נאמנה את שורש Dfs בתיבת הטקסט Comment .
Completing The New Root Wizard (השלמת הפעולה של אשף השורש החדש)	סקור את ההגדרות עבור השרת המארח, השיתוף בשורש ושם השורש. לחץ Back אם נדרש לבצע שינויים, או Finish להשלמת הליך ההתקנה.

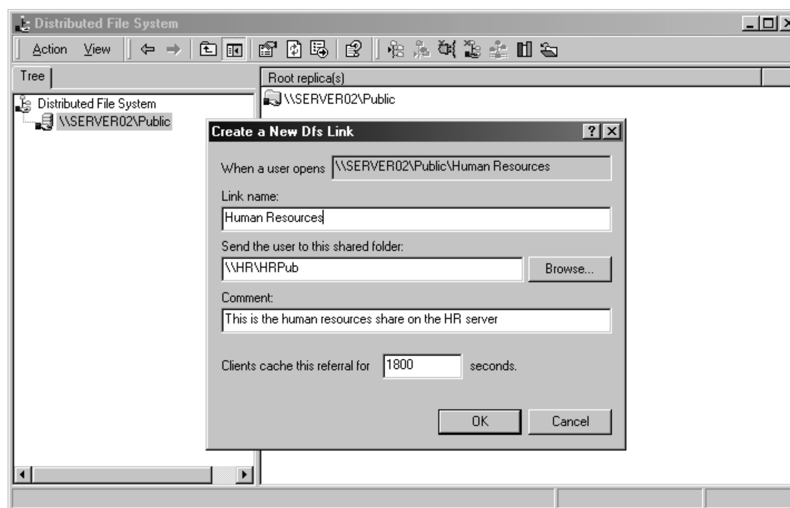
הגדרת Domain Dfs Root

מערכת Domain Dfs Root כותבת את טופולוגיית Dfs ומאחסנת אותה ב-Active Directory. סוג זה של Dfs מאפשר לקישורי Dfs להצביע על תיקיות משותפות רבות (שכפולים) לשם fault tolernace. בנוסף, היא תומכת גם ב-DNS, רמות רבות של Child-Volumes, ושכפול קבצים. ליצירת Domain Dfs Root עם Falut Tolerance, השתמש בכלי Distributed File System להפעלת אשף New Dfs Root.

הגדרת קישורי Dfs

משתמשים יכולים לדפדף בתיקיות הנמצאות תחת שורש Dfs בלי לדעת היכן ממוקמים המשאבים באופן פיסי. לאחר שיצרת שורש Dfs, תוכל ליצור קישורי Dfs (הידועים גם כצמתי-צאצאים).

ליצירת קישור Dfs, פתח את תוסף התוכנה Distributed File System, ולחץ על שורש Dfs אליו תחבר קישור Dfs. בתפריט Action, לחץ על New Dfs Link. תופיע תיבת דו-שיח Create A New Dfs Link כמתואר בתרשים 5.3.



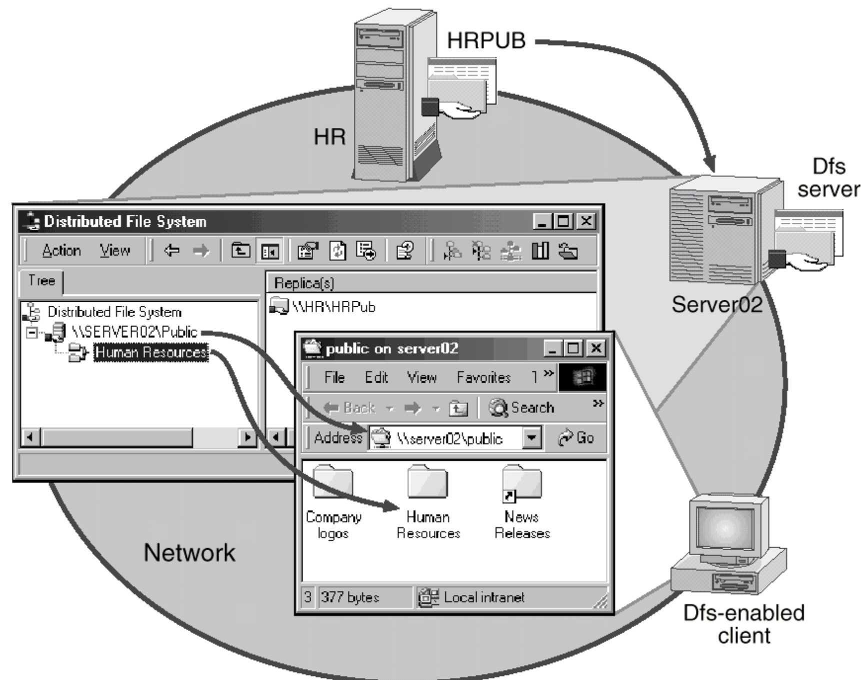
תרשים 5.3 יצירת קישור Dfs חדש משורש Dfs ציבורי לשיתוף במשאבי אנוש.

הטבלה להלן מתארת את האפשרויות בתיבת הדו-שיח:

אפשרות	תיאור
Link Name	השם מתחת לשורש Dfs שמשתמשים יראו כאשר יתחברו ל-Dfs.
Send The User To This Shared Folder	שם UNC של המקום האמיתי של הקובץ המשותף אליו מתייחס קישור Dfs זה. שים לב שהשרת המשמש כאורח של Dfs חייב להיות בעל יכולת גישה לכל תיקיה משותפת אליו מתייחס קישור Dfs זה.
Comment	מידע נוסף (אופציונלי) המסייע במעקב אחר התיקיה המשותפת (לדוגמה, שמה האמיתי של התיקיה המשותפת).
Clients Cache This Dfs Referral For x Seconds	משך הזמן בו לקוחות מעבירים הפניות מקישור Dfs למטמון. עם תום זמן ההפנייה, הלקוח מבצע שאילתה על שרת Dfs אודות מיקום קישור Dfs, אף אם הלקוח יצר כבר קשר עם קישור Dfs.

קישור Dfs יפיע תחת volume root Dfs בכלי Distributed File System ויופיע ל-Client Enabled Dfs כתיקיה מתחת לשורש Dfs.

תרשים 5.4 מציג שורש Dfs בשם Server02\Public\\ וקישור Dfs על שרת אחר.



תרשים 5.4 שורש Dfs וקישור Dfs, כפי שהם מופיעים בתוסף תוכנה Distributed File System, וכיצד הם מוצגים אצל Dfs Enabled Client.

תרגיל 1: יצירת שורש Dfs וקישור Dfs

בתרגיל זה, תגדיר שיתופים, תיצור שורש Dfs עצמאי ואז תיצור קישור Dfs.

הליך 1: יצירת תיקיות ושיתופים

בהליך זה תיצור תיקיות או תשתמש בתיקיות קיימות ותיצור שיתופים עבורן. תוכל להשתמש בכל שיטה שתבחר ליצירת תיקיות ושיתופים או לעקוב אחר השלבים בהליך 1 להלן.

1. הכנס לשרת Server01 בשם משתמש Administrator עם הסיסמה password.
2. פתח את My Computer בשולחן העבודה. חלון My Computer יופיע.
3. פתח דיסק מקומי (:H).

4. מתפריט File, בחר New ואחר כך Folder. תופיע תיקיה New Folder בחלון הדיסק המקומי (:H), והסמן המהבהב יופיע בתיבת New Folder.

5. שנה את שם התיקיה ל-Public.

6. בחר בתיקיה Public, ומתפריט File בחר Sharing. תופיע תיבת דו-שיח Public Properties.

7. בחר בלחצן אפשרויות Share This Folder. בתיבת הטקסט Comment, הקלד **Dfs root share**.

8. לחץ OK. התיקיה Public תופיע עם יד מתחתיה.

9. חזור על שבעת השלבים האחרונים ליצירת התיקיות והשיתופים, המפורטים בטבלה להלן, תוך שימוש בהרשאות ברירת המחדל.

הייה מודע לכך שבמקרים מסוימים, התיקיות ייווצרו באותיות כוננים אחרות מ- :H, ובמקרה אחד שיתוף ייווצר על שרת Server02 בתיקיה שקיימת כבר.

שם מחשב	כונן	תיקיה	שם שיתוף	מטרה/הערה
Server02	C:	\Inetpub\wwwroot	internal	תכולת אינטרנט פנימית
Server01	H:	\Press	press	הודעות לעיתונות
Server01	C:	\Inetpub\ftproot	ftproot	מחיצה ממופית של ספריית שורש FTP
Server01	I:	\dev\TechDocs	TechDocs	אזור מסמכים טכניים
Server01	C:	\Public\Press	PressRepl	העתק הודעות לעיתונות

הליך 2: יצירת Stand-Alone Dfs Root על שרת Server01

בהליך זה תיצור שורש Dfs עצמאי שיארח את השיתופים שיצרת בהליך 1.

1. לחץ על לחצן Start, הצבע על Programs, הצבע על Administrative Tools ולחץ על Distributed File System. תוסף התוכנה Distributed File System יופיע.
2. קרא את ההודעה המוצגת בחלונית הימנית.
3. בתפריט Action, לחץ על New Dfs Root (שורש Dfs חדש). יופיע אשף New Dfs Root.
4. קרא את המידע במסך אשף Welcome To The New Dfs Root Wizard, ולחץ Next.
5. במסך Select Dfs Root Type (בחר בסוג שורש Dfs), שים לב שישנם שני סוגים של Dfs שתוכל ליצור:

   Domain Dfs Root, הכותב את טופולוגיית עץ Dfs ל- Active Directory store ותומך ב- DNS ושכפול קבצים.

   Stand Alone Dfs Root, שאינו משתמש ב-Active Directory Services ואינו תומך בשכפול קבצים אוטומטי.

   כיון שלא הגדרת Domain Controller בשלב זה של לימודיך, צור Stand Alone Dfs Root.
6. בחר בלחצן אפשרויות Create A Stand-Alone Dfs Root, ולחץ Next.
7. במסך Specify The Host Server For The Dfs Root, ודא ששרת Server01 מוצג, ולחץ Next.

   במסך Specify The Dfs Root Share (הגדר את שיתוף שורש Dfs), הגדר את השיתוף שיצרת בהליך 1.

   שים לב שניתן להשתמש בשיתוף קיים עבור שורש Dfs, או שהאשף יוכל ליצור תיקיה משותפת חדשה עבורך.
8. ודא שלחצן אפשרויות Use An Existing Share (השתמש בשיתוף קיים) מסומן, ומהתפריט הנפתח בחר Public.
9. לחץ Next.
10. בתיבת הטקסט Comment, המופיעה במסך Name The Dfs Root (תן שם לשורש Dfs), הקלד **Public Access Share**, ולחץ Next.
11. עיין בהגדרות המופיעות במסך אשף Completing The New Dfs Root Wizard (אשף השלמת שורש Dfs חדש), ולחץ Next.

    תוסף התוכנה Distributed File System יופיע ותצורת שורש Dfs בשרת SERVER01 היא Public.

הליך 3: יצירת קישורי Dfs

בהליך הבא תיצור קישורי Dfs תחת השורש \\SERVER01\Public.

1. בחלונית השמאלית של תוסף התוכנה Distributed File System, בחר \\SERVER01\Public.
2. פתח את תפריט Action, ושים לב שאפשרויות New Root Replica (העתק שורש חדש) ו-Replication Policy (מדיניות שכפול), אינם זמינים.
3. לחץ על New Dfs Link (קישור Dfs חדש). תיבת הדו-שיח Create A New Dfs Link (צור קישור Dfs חדש) תופיע.
4. בתיבת הטקסט Link Name, הקלד **intranet**.
5. לחץ Browse (עיון). חלון Browse For Folder (עיין לאיתור תיקיה) יופיע.
6. הרחב את סימן + שנמצא משמאל לכיתוב Computers Near Me.
7. הרחב את סימן + הנמצא משמאל לכיתוב Server02, לחץ Internal, ולחץ OK.

   בתיבת הטקסט Send The User To This Shared Folder (שלח את המשתמש לתיקיה משותפת זו), תופיע ההפניה \\Server02\internal.
8. בתיבת הטקסט Comment, הקלד **Internal Web content**, ולחץ OK.
9. תמיד התחל שלב זה על ידי לחיצה על \\SERVER01\Public בתוסף התוכנה של Distributed File System, וחזור על שלבים 3-8 ליצירת קישורי Dfs חדשים תוך שימוש במידע המופיע בטבלה להלן:

שם קישור	שלח את המשתמש לתיקיה משותפת זו	הערה
news	\\Server01\Press	הודעות עדכניות לעיתונות
ftp	\\Server01\ftproot	ספריית שורש FTP
tech	\\Server01\TechDocs	אזור מסמכים טכניים

הערה במקום לדפדף לאיתור שיתוף, תוכל להכניס את שם השרת והשיתוף בתחביר UNC סטנדרטי.

הליך 4: יצירת העתק של Dfs

בהליך הזה, תיצור העתק של קישור News Dfs (חדשות). קישור Dfs זה מפנה לתיקיה H:\Press המשותפת כ-Press, וההעתק יאוחסן בתיקיה C:\Public\Press, המשותפת כ- PressRepl.

הערה כיון שיצרת קישור Dfs עצמאי, יש להעתיק ולהתאים את הקבצים בצורה ידנית בין שתי התיקיות. שירות שיכפול קבצים אינו זמין עבור העתקים שנוצרו בקישור Dfs עצמאי.

---

1. בחר בקישור News בחלונית השמאלית של תוסף התוכנה Distributed File System.
2. בתפריט Action, לחץ על New Replica. תיבת דו-שיח Add A New Replica (הוסף העתק חדש) תופיע.
3. בתיבת טקסט Send The User To This Shared Folder, הקלד **\\\\SERVER01\PressRepl**. שים לב שלא ניתן להגדיר מדיניות שכפול עבור העתק זה.
4. לחץ OK. בחלונית הימנית, יופיעו גם השרת \\\\SERVER01\Press וגם השרת \\\\SERVER01\PresRepl.

הליך 5: גישה ל-Dfs בשרת Server01

בהליך זה תשתמש בקובץ האצווה המסופק עם הספר להעתקת קבצים לקישורי Dfs שנוצרו בנהלים הקודמים. לאחר העתקת הקבצים, גש אליהם באמצעות סייר Windows.

חשוב קבצי האצווה המסופקים עם ספר זה יעבדו כנדרש רק אם שני השרתים פועלים, השיתופים נוצרו בדיוק כמפורט בתרגיל זה, וסיסמת חשבון המנהל (Administrator) בשני המחשבים היא password.

---

1. הכנס את התקליטור המצורף לספר זה לכונן התקליטורים של Server01.
2. פתח את כונן התקליטורים מ-My Computer.
3. פתח את תיקיה \Books\59279\chapt05\ex1.
4. לחץ על קובץ האצווה ex1copy.bat, ומתפריט File, לחץ Open.

   חלון שורת פקודה ייפתח בעוד קבצים מועתקים לקישורי Dfs. בסיום תהליך ההעתקה החלון ייסגר.

   השלם את כל השלבים הנותרים בהליך זה בשרת Server02.

5. כדי לגשת לשורש Dfs העצמאי בשרת Server01 משרת Server02, פתח את My Network Places (מיקומי הרשת שלי), ואז פתח את Computers Near Me (מחשבים סמוכים אלי). יופיע חלון Computers Near Me ובו כל המחשבים בקבוצת העבודה.

6. לחץ על Server01, ומתפריט File, לחץ Open.

יופיעו כל השיתופים ושורש Dfs (Public) יחד עם אובייקטים אחרים על שרת Server01. שים לב שהתיקיה Public מופיעה ככל שיתוף אחר על שרת Server01.

7. לחץ על התיקיה Public, ומתפריט File, לחץ Open. יופיעו ארבעת קישורי Dfs שנוצרו בהליך הקודם.

8. פתח כל תיקיה וודא שהקבצים הבאים נוכחים:

תיקיה	קובץ/ים
ftp	dirmap.txt ,dirmap.htm
intranet	Q240126 - Best Practices for Using Sysprep with NTFS Volumes.htm
news	press.wri
tech	RFS 1777.txt ,Dfsnew.doc

שים לב שהתיקיה intranet תכיל קבצים נוספים, כיון שתיקיה זו מפנה לספריה שנוצרה בעת התקנת Windows 2000 Server.

9. איזו תיקיה מייצגת מיקום בשרת אחר, שאינו Server01?

10. איזו תיקיה מייצגת כונן שנטען לתיקיה שהיתה ריקה בעבר?

11. מוקדם יותר בתרגיל זה, יצרת העתק של קישור Press של Dfs. שם ההעתק הוא \\SERVER01\PressRepl. קישור Dfs זה הוא תיקיה משותפת בשם PressRepl והיא מותקנת ב-C:\Public\Press. אם תעיין בתכולת ספריה זו, תמצא שהיא ריקה. אולם כאשר תעיין בקישור News של Dfs, תמצא שיש קובץ בשם Press.wri. מדוע העתק Dfs של PressRepl ריק?

טיפ תוכל להשתמש בתוסף תוכנה Distributed File System לבדיקת מצבו של קישור Dfs, ולפתוח חלון לתכולת הקישור.

סיכום שיעור

Dfs מספקת אמצעי נוח למשתמשים לגישה לתיקיות משותפות המבוזרות על פני הרשת כולה. קובץ שיתוף Dfs בודד, בשם שורש Dfs, משמש כנקודת גישה לתיקיות משותפות אחרות ברשת, הנקראות קישורי Dfs. Dfs מארגנת תיקיות משותפות במחשבים שונים ברשת למערכת היררכית לוגית יחידה. Dfs מסייעת בניווט ברשת ובניהול, בעודה שומרת על הרשאות הרשת. ניתן להגדיר שני סוגים של שורשי Dfs במערכות Windows 2000 Server : Stand-Alone Dfs Root, ו-Domain Dfs Root. הסוג הראשון, Stand Alone Dfs Root מאחסן את טופולוגיית Dfs על מחשב בודד. סוג זה של Dfs אינו מספק Fault tolerance אם המחשב, המאחסן את טופולוגיית Dfs או כל תיקיה משותפת בה משתמש Dfs, נכשל. Domain Dfs Root כותב את טופולוגיית Dfs ל- Active Directory Store. סוג זה של Dfs מאפשר לקישורי Dfs להפנות לתיקיות משותפות רבות זהות ותומך בשכפול קבצים לצורך Fault tolerance. בנוסף, הוא תומך ב-DNS ורמות רבות של קישורי Dfs. Dfs משתמש ב-FRS לשכפול נתונים ב-Domain Dfs Roots וקישור domain של Dfs. כאשר נעשים שינויים לקישור Dfs שהוא חלק משורש Domain, השינויים משוכפלים אוטומטית לחברים האחרים של ההעתק.

שיעור 2:
FRS - File Replication Service

FRS - **F**ile Replication **S**ervice הוא שירות שכפול הקבצים במערכת Windows 2000 Server. הוא משמש להעתקה ותחזוקת קבצים במספר שרתים בו-זמנית ולשכפול volume Windows 2000 system (SYSVOL), בכל Domain Controllers. בנוסף ניתן להגדיר לו שכפול קבצים מ-Domain Dfs Root.

לאחר שיעור זה, תוכל

- לתאר איזה נתונים ניתן להעתיק עם FRS.
- להגדיר שכפול עבור Domain Dfs Roots.
- לתאר את הליך השכפול ב-Active Directory Services ו-FRS.

זמן לימוד משוער: 25 דקות

שכפול FRS

FRS מותקן אוטומטית על כל שרתי Windows 2000 Server. הוא מוגדר להתחיל אוטומטית בכל ה-Domain Controllers ולהתחיל ידנית בכל שרת עצמאי או בשרתים חברים. אף ששכפול Active Directory ו-FRS אינם קשורים זה לזה, יש להם טופולוגיה, מונחים, ושיטות זהים. למעשה, Active Directory משתמש ב-FRS לתאם את המדריך בין כל בקרי התחומים.

לכל Windows 2000 Domain יש שרת אחד או יותר המשמשים כ-Domain Controllers. כל DC מאחסן העתק מושלם של Active Directory עבור ה-domain שלו, והוא מעורב בניהול שינויים ועדכונים ב-Directory.

בתוך אתר, מכלול Active Directory Services יוצר אוטומטית טופולוגיה טבעתית לשכפול בין Domain Controllers באותו domain. הטופולוגיה קובעת את הנתיב כך שעדכוני ה-Directory יזרמו מ-DC אחד למשנהו, עד שכל ה-DCs יקבלו את עדכוני ה-directory.

המבנה הטבעתי מבטיח שיש לפחות שני נתיבי שכפול בין DC אחד למשנהו; אם DC אחד אינו פעיל זמנית, השכפול עדיין ממשיך בכל שאר ה-Domain Controllers.

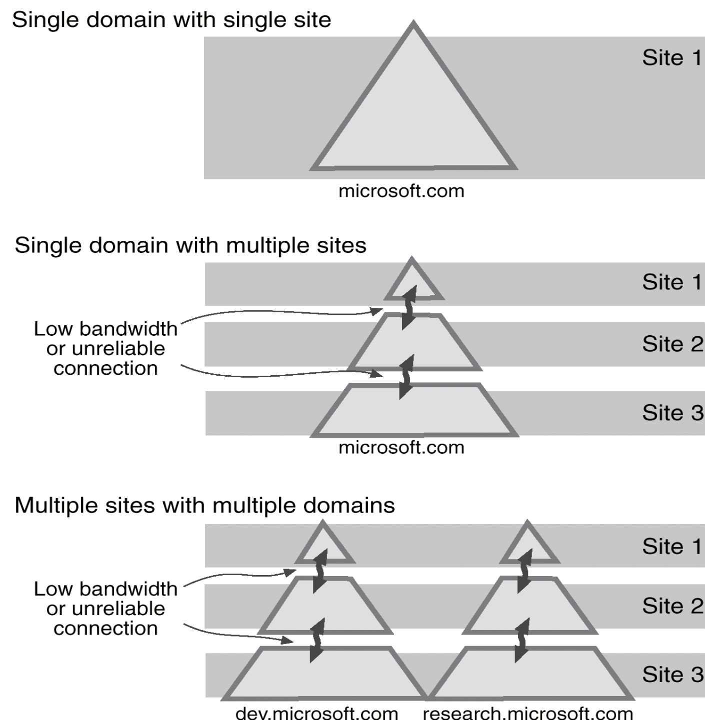
מכלול Active Directory Services משתמש בשכפול Multimaster Replication, שבו אף Domain Controller בודד אינו master; אלא, כל ה-Domain Controllers בתוך Domain הם שווי ערך.

מכלול Active Directory Services מנתח תקופתית את טופולוגיית השכפול באתר כדי לוודא שהיא עדיין יעילה. אם תוסיף או תסיר Domain Controller מרשת או אתר, מכלול Active Directory Services חוזר ומגדיר את הטופולוגיה כדי שתשקף את השינוי.

אתרים ושכפולים

אתר (Site) מורכב מ-IP Subnet אחת או יותר, המזהה קבוצה של מחשבים מחוברים בקשר מהיר. יש לשלב רק Subnets בהן חיבורי הרשת מהירים ואמינים, במהירות של 512Kbps לפחות.

מבנה domain ומבנה Site נשמרים בנפרד ב-Active Directory Services. Domain בודד יכול להכיל אתרים רבים, ואתר בודד יכול להכיל Domains רבים או חלקים מ-Domains, כמתואר בתרשים 5.5.



תרשים 5.5 Domain בודד עם אתר בודד, Domain בודד עם אתרים רבים, ואתרים רבים עם Domains.

ישנם שני סוגים של שכפול: שכפול Intra-Site ושכפול Inter-Site.

שכפול Intra-Site

מאפייני שכפול Intra-Site הם:

- ❖ שכפול Intra-Site מתבצע בין Domain Controllers בתוך אתר.
- ❖ נתונים משוכפלים אינם נדחסים.
- ❖ מרווח זמן ברירת המחדל של השכפול הוא חמש דקות.
- ❖ השכפול הוא מבוסס אירוע (Trigger-Based), כלומר מתבצע מייד לאחר קבלת הודעה לביצוע.

שכפול Inter-Site

מאפייני שכפול Inter-Site הם:

- ❖ שכפול Inter-Site מתבצע בין Domain Controllers באתרים שונים.
- ❖ תוכל להגדיר את הזמן בו אמור להתרחש שכפול Inter-Site. מרווח ברירת המחדל של זמן השכפול הוא שלוש שעות.
- ❖ תוכל לקבוע ששכפול Inter-Site ייעשה באמצעות תעבורת הרשת.
- ❖ שכפול Inter-Site נדחס, ללא תלות באמצעי התעבורה.
- ❖ דחיסת שכפול Inter-Site מצמצמת את נפח המידע ב- 88 עד 90 אחוז.

חסרון אחד של שכפול Inter-Site הוא, שהוא אינו מוגדר אוטומטית; הוא חייב להיות מוגדר על ידי ה-Administrator.

KCC - Knowledge Consistency Checker

בתוך אתר, יוצר הליך בשם KCC טופולוגיה טבעתית לשכפול בין Domain Controllers באותו Domain. הטופולוגיה הנוצרת מגדירה נתיבים לעדכוני Directories כך שיוזרמו מ-DC אחד לשני עד שכל ה-DCs קיבלו את עדכוני ה-Directory.

המבנה הטבעתי מבטיח שיהיו לפחות שני נתיבי שכפול מ-DC אחד למשנהו, כך שאם DC אחד אינו פעיל זמנית, השכפול יימשך בכל שאר ה-DCs (בניגוד לטופולוגיית Ring פיזית). בנוסף, המבנה הטבעתי הוא כזה שעדכון כרוך במקסימום שלוש "קפיצות" (Hops) מ-DC, שהוא מקור העדכון, לכל DC אחר באתר.

ה-KCC מנתח מדי פעם את טופולוגיית השכפול באתר לוודא שהיא יעילה. אם מוסיפים או מסירים Domain Controller מהרשת או מאתר, KCC חוזר ומגדיר את הטופולוגיה לשקף את השינוי.

הערה Administrators יכולים לעשות שינויים והתאמות לטופולוגיית השכפול, כולל שינוי לוח הזמנים לשכפול Inter-Site, כדי לענות על דרישות הארגון.

USN - Unique Sequence Number

כאשר מתבצע עדכון של אובייקט directory ב-Domain Controller, בין אם הדבר קורה עקב שינוי שעשה משתמש או Administrator ובין אם על ידי שכפול מ-DC אחר, ה-Domain Controller משייך USN (מספר רצף ייחודי) לשינוי. כל Domain Controller שומר על USN של עצמו ומחיל USN מצטברים לכל שינוי ב-Directory שבוצע ב-Domain Controller .

כאשר Domain Controller כותב את השינוי ב-Directory, הוא כותב גם את המספר המצטבר הייחודי עם התכונה.

כל Domain Controller מתחזק טבלה של ה-USN שהוא מקבל מכל Domain Controller אחר ב-Domain, והטבלה רושמת את ה-USN הגבוה ביותר המתקבל מכל Domain Controller. כל Domain Controller מודיע מדי פעם לשאר Domain Controllers ב-domain שהוא קיבל שינויים, ושולח את ה-USN הנוכחי שלו. כל Domain Controller שמקבל את ההודעה בוחן את טבלת USN של עצמו אחר USN האחרון שהתקבל מ-Domain Controller השולח. אם יש שינויים, ו-Domain Controller לא קיבל אותם, הוא מבקש שיישלחו רק השינויים.

שימוש ב-USN מבטל את הצורך בחותמות זמן מדויקות לשינויים ובסינכרון מדויק של זמן בין Domain Controllers ב-Domain. אולם, חותמות זמן עדיין מוחלות על שינויי directory, לקביעת עדיפות במצבי שוויון.

השימוש ב-USN מפשט גם התאוששות מכשל. כש-DC פועל שנית לאחר כשל, הוא חוזר ומתחיל שכפול, על ידי כך שהוא שואל את כל שאר ה-DCs אודות שינויי USN גדולים מה-USN האחרון של DC זה, המופיע בטבלה של עצמו. כיון שהטבלה מעודכנת באופן אוטומטי תוך כדי יישום השינוי, מחזורי שכפולים אוטומטיים חוזרים וממשיכים בדיוק בנקודה בה הופסקו, ללא אובדן או כפילות עדכונים.

יישום FRS

החלת FRS - **F**ile **R**eplication **S**ervice כרוכה במספר שלבים:

1. שכפול SYSVOL,
2. שכפול שמות Domain Dfs Roots,
3. הגדרת FRS לשכפול Inter-Site.

שכפול SYSVOL

שינויים לספריית systemroot%SYSVOL% בכל Domain Controller, משוכפלים אוטומטית ל-Domain Controllers אחרים באתר. טופולוגיית השכפול וההליך עצמו נפרדים אך זהים לשכפול Active Directory. כאשר Administrator מוסיף, מסיר, או משנה את תוכן התיקיה systemroot%SYSVOL% בכל Domain Controller, שינויים אלה ישוכפלו ל-Domain Controllers אחרים באתר באופן אוטומטי.

מבנה ברירת המחדל של התיקיה הוא כדלקמן:

- %systemroot%\SYSVOL\Sysvol**domain_name**\Policies
- %systemroot%\SYSVOL\Sysvol**domain_name**\Scripts

כל קובץ או תיקיה שיתוספו ל- systemroot%\SYSVOL\Sysvol**domain_name**%, **י**שוכפל אוטומטית.

שכפול Dfs Fualt Tolerance Roots

Dfs משתמשת ב-FRS לשכפול נתונים בקישורי Domain Dfs. כאשר נעשה שינוי לקישור Dfs המהווה חלק מ-Domain Dfs Root, השינויים משוכפלים אוטומטית לחברים האחרים בשכפול.

Dfs ושכפול קבצים תומכים בתכונות הבאות:

- שכפול אדונים-רבים משכפל קבצים ששונו ו-ACL ששונו כאשר קובץ נסגר.
- ניתן לשנות קובץ בכל חבר שכפול.
- רק ל-Windows 2000 NTFS volumes יש אפשרות לשכפל. ניתן לפרסם שיתופים אחרים כחלופות, אך לא מתבצע שכפול.
- השכפול מבוסס יומן.
- השכפול מבוסס על **R**emote **P**rocedure **C**all (RPC, קריאה לשגרה מרוחקת).
- טופולוגיית FRS זהה לטופולוגיית שכפול של Active Directory.

הליך שכפול Dfs מורכב ממספר שלבים:

1. קובץ משתנה. דבר זה מצוין כאשר משתמש סוגר קובץ.
2. NTFS רושם ביומן השינויים של NTFS.
3. FRS עוקב אחר יומן NTFS לשינויים בקישורי Dfs.
4. FRS מוסיף רשומה ליומן של עצמו.
5. FRS יוצר Staging File (קובץ שינויים) של השינוי בקובץ.
6. FRS מחזיק בשינויים, עד שלוח הזמנים מורה לו לשכפל.
7. היעד מושך את ה- Staging File (קובץ השינויים) ומיישם את הקבצים החדשים.

הוספת Replica Dfs Root Servers

כל שורש Dfs או קישור יכול להתייחס לערכת משאבים משותפים משוכפלים. לקוחות Dfs יבחרו אוטומטית את השכפול הקרוב ביותר, בהתבסס על נתוני טופולוגיית האתר.

להוספת שרתי Dfs משוכפלים ל-Domain Dfs Root או קישור, לחץ לחיצה ימנית על שורש Dfs בכלי Distributed File System, לחץ New, ולחץ Root Replica. הכנס את נתיב UNC עבור ההעתק והשיתוף.

Enabling Dfs Replication

ברירת המחדל היא ששכפול Dfs מבוטל. כדי שיתאפשר שכפול, לחץ לחיצה ימנית על שורש Dfs או קישור Dfs בתוסף התוכנה Distributed File System, ואז בחר Replication Policy. האר וסמן כל שרת בערכת השכפול שברצונך שישתתף בשכפול FRS, ולחץ על לחצן Enable. שרתים שאינם משתתפים בשכפול, צריך לסנכרן ידנית.

הגדרת FRS לשכפול Inter-Site

ניתן להגדיר שכפול Inter-Site על ידי שימוש בתוסף התוכנה Active Directory Sites and Services. להגדרת מאפייני FRS, עליך ליצור קישור אתר חדש עבור פרוטוקול התעבורה Inter-Site שברשימת חלון Tree. ברגע שיצרת את קישור האתר, לחץ לחיצה ימנית על אובייקט קישור האתר ולחץ Properties. תיבת הדו-שיח Properties תיפתח. עתה תוכל להגדיר את שכפול Inter-Site כנדרש.

סיכום שיעור

FRS הוא שירות העתקת הקבצים האוטומטי במערכת Windows 2000 Server. השירות מעתיק ומתחזק קבצים על שרתים רבים. ישנם שני סוגי שכפול: שכפול Intra-Site ושכפול Inter-Site. Site (אתר) מוגדר כתת רשת אחת או יותר המציינת קבוצה של מחשבים מחוברים. בתוך אתר, הליך בשם KCC יוצר טופולוגיה טבעתית באופן אוטומטי לשכפול בין Domain Controllers באותו domain. החלת FRS מורכבת ממספר שלבים, כולל שכפול SYSVOL, שכפול שורשי Dfs של תחומים והגדרת FRS.

הערה Domain Dfs Roots **ו-**FRS **יותקנו בפרק הבא לאחר שמכלול** Active Directory Services כבר פועל.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות לשאלה, עיין בשיעור המתאים ונסה לענות על השאלה שוב. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

The following questions are intended to reinforce key information presented in this chapter. If you are unable to answer a question, review the appropriate lesson and then try the question again. Answers to the questions can be found in Appendix A.

1. How does a mounted drive to an empty folder differ from a Dfs root?
2. In Exercise 1, you were asked to notice that New Root Replica and Replication Policy were not available options in the Distributed File System snap-in. Explain why these options are not available.
3. Why doesn't Dfs directly provide a security infrastructure?
4. How is the KCC involved in maintaining Active Directory store synchronization between domain controllers?
5. What data does the FRS replicate?

1. מה השוני בין כונן הנטען בתיקיה ריקה לשורש Dfs?
2. בתרגיל 1, נתבקשת לשים לב ש-New Root Replica ו-Replication Policy אינן אפשרויות זמינות בתוסף התוכנה Distributed File System. הסבר מדוע אפשרויות אלה אינן זמינות?
3. מדוע Dfs אינם מספקים מבנה אבטחה באופן ישיר?
4. איך KCC משתלב בתחזוקת סינכרון Active Directory בין Domain Controllers?
5. מה משכפל ה- FRS?

פרק 6

Active Directory Services

אודות פרק זה

בפרק 1, הוצגו בפניך המושגים הבסיסיים של Active Directory Services. הצגה זו כללה דיון על כמה מתכונות Active Directory, כגון יכולת הגידול המובנית ותמיכת תקנים פתוחה, והמשיכה בדיון אודות המבנים הלוגיים והפיסיים של Active Directory store. פרק 6 מרחיב בנושא ארכיטקטורת Active Directory, מסביר כיצד להתכונן ליישום Active Directory Services בסביבת Windows 2000, ואיך לבצע זאת באופן מעשי. לבסוף, הפרק דן בניהול מכלול Active Directory Services לאחר שיושם בסביבת Windows 2000.

לפני שתתחיל

לביצוע השיעורים בפרק זה נדרש:

- ❖ מערכת Windows 2000 Server מותקנת ופועלת על Server01 כמתואר בפרק 2, תרגיל 1.
- ❖ מחשב שני מחובר ברשת ל-Sever01 ופועל תחת מערכת הפעלה Windows 2000 Server, כמתואר בפרק 3, תרגיל 1.
- ❖ תקליטור התקנה של Windows 2000 Server.

שיעור 1: סקירת Active Directory Services

מכלול Active Directory Services הוא שירות ספריית רשת פעילה הנכלל במערכת Windows 2000 Server. הוא מרחיב את תפקודיות Directory Services (שירותי ספריית הרשת) הקודמים מבוססי Windows ומוסיף תכונות חדשות. מכלול Active Directory Services הוא מערכת מאובטחת, מבוזרת, מחולקת למחיצות משוכפלת. הוא מתוכנן לעבוד היטב בכל גודל התקנה, משרת בודד עם מספר מאות אובייקטים, עד אלפי שרתים עם מיליוני אובייקטים. מכלול Active Directory Services מוסיף תכונות חדשות רבות המאפשרות ניווט קל וניהול כמויות נתונים גדולות, ובכך חוסך זמן למשתמשים ו-Administrators גם יחד.

לאחר שיעור זה, תוכל

- לתאר את המושגים ומבנה Active Directory Services.

זמן לימוד משוער: 40 דקות

מבוא ל-Active Directory Services

שירותי Active Directory משולבים לחלוטין עם Windows 2000 Server ומאפשרים מבט הירכי, יכולת הרחבה, גידול ואבטחה מבוזרת, הנדרשים על ידי לקוחות עסקיים. Active Directory Services מאפשרים ל-Administrators, מפתחים ומשתמשים לקבל גישה לשירות ספריית הרשת המשולב באופן מושלם בסביבות אינטרנט ואינטראנט גם יחד. Active Directory Services הם חלק קריטי במערכת המבוזרת. הם מאפשרים ל-administrators ומשתמשי קצה להשתמש בשירותי ספריית הרשת כמקור מידע, בנוסף להיותם שירות ניהול.

מכלול Active Directory Services משלב את מושג ה-Namespace (טווח שמות) של האינטרנט עם Directory Services (שירות ספריית הרשת) של מערכת ההפעלה. **Namespace** (טווח שמות) הוא אוסף נתונים מובנה בו ניתן להשתמש בשמות לייצוג סמלי של סוגים אחרים של נתונים, כגון שם מארח המייצג כתובת IP, ואשר בו הוגדרו חוקים ייחודיים הקובעים כיצד ליצור ולהשתמש בשמות. השילוב של המושג **Namespace** עם Directory Services מאפשר לארגונים לאחד ולנהל Multiple nsamespace הקיימים היום בסביבות ההטרוגניות של תוכנה וחומרה ברשתות ארגונים. מכלול Active Directory Services משתמש ב-**L**ightweight **D**irectory **A**ccess **P**rotocol (LDAP), פרוטוקול מצומצם לגישה לספריית הרשת) כפרוטוקול הליבה, והוא יכול לחצות גבולות מערכות הפעלה, תוך שילוב טווחי שמות רבים. הוא מסוגל לנהל ספריות רשת יישומים ייעודיים, בנוסף לספריות רשת מבוססי NOS אחרים, לאספקת ספריית רשת למטרות כלליות שיכולה להפחית את מעמסת הניהול והעלויות שהן חלק ממטלות תחזוקת טווחי שמות רבים.

מכלול Active Directory Services אינו X.500 Directory. במקום זאת, הוא משתמש ב-LDAP כפרוטוקול הגישה, ותומך במודל נתונים X.500 מבלי לדרוש ממערכות שיארחו את כל מכלול מערכת X.500. התוצאה היא יכולת רב-תפקודית ברמה גבוהה (Hign Level of Interoperability), התומכת ברשתות הטרוגניות.

הערה למידע נוסף אודות האופן בו LDAP משתמש ב- X.500, פנה לתקליטור המצורף לספר זה (\chapt01\articles\RFC1777.TXT\)

מכלול Active Directory Services מאפשר נקודת ניהול יחידה עבור כל המשאבים הקיימים, כגון קבצים, ציוד היקפי, חיבורי Hosts (מחשבים מארחים), מסדי נתונים, גישה לאינטרנט, משתמשים ואובייקטים אחרים. Active Directory Servoices משתמשים בשיטת שמות **D**omain **N**ame **S**ystem - DNS לאיתור, מארגנים אובייקטים בתוך domains בהירכיה של יחידות ארגוניות (**O**rganizational **U**nits - OU), ומאפשרים חיבור מספר domains במבנה עץ. הניהול הופך פשוט אף יותר, מכיון שכבר לא קיים מבנה **P**rimary **D**omain **C**ontroller (PDC, בקר תחומים ראשי) או **B**ackup **D**omain **C**ontroller (BDC, בקר תחומים לגיבוי), כפי שיושם ב-Windows NT Server. במקום זאת, שירותי Active Directory משתמשים ב-Domain Controllers בלבד, וכל ה-Domain Controllers הם שוויוניים. Administrator יכול לעשות שינויים ולעדכן בכל Domian Controller, והעדכונים ישוכפלו בכל שאר ה-DCs.

הערה למידע נוסף על תכונות, מושגים ומבנה Active Directory, פנה לתקליטור המצורף לספר זה (\chapt06\articles\RFC1777.txt\) תיקיה זו כוללת שלושה מאמרים המרחיבים בנושאים אלה:

- Managing The Active Directory.doc
- Active_Directory_Technical_summary.doc
- Active_Directory_DS_Strategy.doc

הבנת מושגי Active Directory

קיימים מספר מושגים חדשים הקשורים ב-Active Directory Services. חלק מהמושגים עשויים להיות מוכרים, בעוד לאחרים עשויה להיות משמעות שונה מהמקובל. הסעיפים להלן מתארים חלק ממושגים אלה, כולל Extensible Schema (סכמה הניתנת להרחבה), Global Catalog (קטלוג גלובלי), Namespace (טווח שמות), ו- Naming Conventions (מוסכמות למתן שמות).

Extensible Schema

הסכמה של Active Directory כוללת הגדרה רשמית של תכולת שטח אחסון Active Directory ומבנהו, כולל כל המאפיינים (Attributes), סיווגים (Classes) ותכונות סיווגים (Class Properties). עבור כל סיווג אובייקט, מגדירה הסכמה (Schema) את המאפיינים שחייבים להיות לאותו סיווג, את המאפיינים שניתן להוסיף לאותו סיווג, ואיזה סיווג אובייקט יכול לשמש כהורה של סיווג האובייקט הנוכחי.

התקנת Active Directory Services על Domain Controller הראשון ברשת, יוצרת Default Schema (סכמת ברירת מחדל). סכמת ברירת המחדל מכילה הגדרות של אובייקטים ותכונות משותפות נפוצות, כגון משתמשים, מחשבים, מדפסות וקבוצות. בנוסף, Default Schema כוללת גם הגדרות של אובייקטים ותכונות פנימיות בהם משתמש מכלול Active Directory Services לפעולתו.

הסכמה של Active Directory ניתנת להרחבה (Extensible). המשמעות היא שניתן להגדיר סוגי אובייקטים ומאפיינים חדשים ב-Directory (ספריית הרשת), ומאפיינים חדשים לאובייקטים קיימים. הסכמה מיושמת ומאוחסנת ב-Active Directory Store עצמו (הנמצא ב-Global Catalog) וניתן לעדכנה באופן דינמי. אי לכך, יישום יכול להרחיב את הסכמה עם מאפיינים וסיווגים חדשים, והיא יכולה להשתמש בהרחבות מייד.

Extending the Schema

הרחבת הסכמה של Active Directory היא פעולה מתקדמת המיועדת למתכנתים ומנהלי רשתות מנוסים.

אזהרה Extending the Schema היא פעולה רגישה ביותר, עם השלכות אפשריות על הרשת כולה. יש להרחיב Shema באמצעות תכנות, ורק כאשר ההרחבה חיונית. שינויי Shema שגויים עלולים להפריע או לשתק את Windows 2000 Server, ואף ייתכן שאת הרשת כולה.

Global Catalog

הקטלוג הגלובלי (Global Catalog) הוא מילון (Repository) המידע המרכזי אודות אובייקטים ב-Domains Tree (אוסף Domains היוצרים היררכיית Domains) או ב-Forest (אוסף Domains Tree המהווים חלק מהיררכיות שונות). מכלול Active Directory Services יוצר את תוכן הקטלוג הגלובלי מהתחומים המהווים חלק מה-Directory (ספריית הרשת) באמצעות הליך השכפול הרגיל. מערכת השכפול (Replication System) של Active Directory בונה את הקטלוג הגלובלי באופן אוטומטי ויוצרת את טופולוגיית השכפול.

הקטלוג הגלובלי הוא שירות, בנוסף להיותו מקום אחסון פיסי, המכיל העתק של מאפיינים נבחרים של כל אובייקט ב-Active Directory Store. הליך השכפול החלקי מאפשר מתן תשובות לרבות מהשאילתות הנפוצות ישירות מהקטלוג הגלובלי, ללא צורך בחיפוש ב-Domain המקור. ברירת המחדל היא שמאפיינים המאוחסנים בקטלוג הגלובלי הם אלה שמשמשים לעיתים הקרובות ביותר בפעולות חיפוש (כגון שמות פרטיים ומשפחה של משתמש, שם כניסה למערכת וכו') ואלה המשמשים לאיתור העתק מלא של האובייקט. עקב כך, ניתן להשתמש בקטלוג הגלובלי לאיתור אובייקטים בכל מקום ברשת, ללא צורך בשכפול כל נתוני ה-Domain בין ה-Domain Controllers.

הערה תוכל להשתמש בתוסף תוכנה Active Directory Schema להגדיר איזה מאפיינים ייכללו בשגרת השכפול של הקטלוג הגלובלי. תוסף תוכנה זה נמצא ב-%systemroot%\system32 ושמו Schmmgmt.msc. **יש להשתמש בכלי זה בזהירות. רצוי ומומלץ שרק מתכנתים מנוסים או מנהלי רשתות מנוסים, המבינים את הסכמה ואופן פעולתה, ישתמשו בכלי זה.**

בעת התקנת Active Directory Services על Domain Controller הראשון, DC זה הוא, כברירת מחדל, Global Catalog Server. שרת קטלוג גלובלי הוא Domain Controller המאחסן העתק של הקטלוג הגלובלי. התצורה של שרת הקטלוג הגלובלי הראשונית צריכה להיות בעלת יכולת תמיכה בכמה מאות אלפים עד מיליון אובייקטים, אם אפשרות גידול.

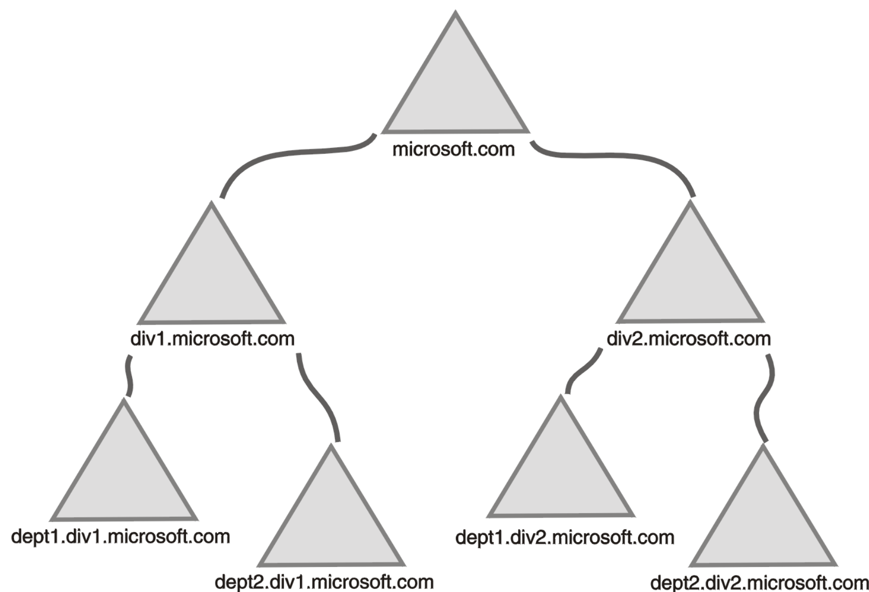
ניתן להגדיר גם Domain Controllers נוספים כשרתי קטלוג גלובליים על ידי שימוש בתוסף התוכנה Active Directory Sites and Services. ההחלטה איזה Domain Controllers להגדיר כשרתי קטלוג גלובליים, צריכה להיות מבוססת על היכולת של מבנה הרשת לטפל בתעבורת שכפולים ושאילתות. ככל שיהיו יותר שרתי קטלוג גלובליים, כך תגדל תעבורת השכפול. אולם, זמינות שרתים נוספים יוצרת תגובה מהירה יותר לשאילתות משתמשים. מומלץ שלכל אתר (Site) מרכזי בארגון יהיה שרת קטלוג גלובלי.

Namespace

מכלול Active Directory Services, כמו כל שירותי Directory, הוא בעיקרו Namespace (טווח שמות). Namespace הוא כל אזור תָחום בו ניתן להשתמש בשם. שימוש בשם הוא ההליך של המרה והחלת השם על אובייקט כלשהו, או מידע שהשם מייצג. טווח השמות של Active Directory מבוסס על מתן שמות בסכמת DNS, המאפשרת שימוש גם בטכנולוגיות אינטרנט. דוגמה של Namespace מובאת בתרשים 6.1.

שימוש ב-Common Namespace מאפשר לאחד ולנהל סביבות תוכנה וחומרה ברשת. יש שני סוגים של טווחי שמות:

- ❖ **Contiguous namespace** (טווח שמות רציף) – שם של Child-object בהיררכיית אובייקטים כולל תמיד את השם של ה-Parent-domain. עץ הוא טווח שמות רציף.
- ❖ **Disjointed namespace** (טווח שמות בלתי-מקושר) – השמות של Parent object ושל Child של אותו Parent object אינם מתייחסים ישירות זה לזה. יער הוא טווח שמות בלתי-מקושר (Disjointed).



תרשים 6.1 .Namespace diagram of a sample domain

מוסכמות למתן שמות

כל אובייקט ב-Active Directory store מזוהה על ידי שם. מכלול Active Directory Services משתמש במיגוון מוסכמות למתן שמות:

- שמות ייחודיים (Distinguished Names),
- שמות ייחודיים יחסיים (Relative Distinguished Names),
- מזהים ייחודיים גלובליים (Globally Unique Identifiers),
- שמות משתמש עיקריים (User Principal Names).

מכלול Active Directory Services הוא Directory service תואם-LDAP, שמשמעו - שכל גישה לאובייקטים של ה-Directory מתרחשת דרך LDAP. LDAP דורש ששמות אובייקטים של ה-Directories יהיו תואמים לתקן RFC - **R**equest **F**or **C**omments, שהוא תקן לשמות אובייקטים ב-Directory Service מסוג LDAP.

Distinguished Name

אובייקטים ממוקמים ב-Active Directory Domain בהתאם לנתיב היררכי, הכולל את תוויות השם של Active Directory Domain, ואת כל אחת מרמות של Container objects. לכל אובייקט ב-Active Directory יש **D**istinguished **N**ame (DN, שם ייחודי)**.** DN מזהה את האובייקט באופן ייחודי וכולל די מידע כדי שלקוח יוכל לאחזר את האובייקט מספריית הרשת. DN כולל את שם ה-domain האוחז את האובייקט, כולל הנתיב המלא דרך הירכיית המכולה עד לאובייקט.

הדוגמה הבאה היא DN המזהה את אובייקט המשתמש James Smith ב-domain microsoft.com:

CN=James Smith, CN=Users, DC=Microsoft, DC=COM

התוחמים (Delimiters) והערכים המשמשים ב-DN עבור James Smith מזוהים בטבלה הבאה:

LDAP Delimeter	Value	Represent
DC	COM	Domain Component
DC	Microsoft	Domain Component
CN	Users	Common Name
CN	James Smith	Common Name

שים לב שתוספי התוכנה של Active Directory אינם מציגים את הקיצור של LDAP (CN=, DC=, O=). קיצורים אלה מוצגים רק כדי להראות כיצד LDAP מזהה חלקים בשם הייחודי. חלק ממאפייני השמות המתוארים ב-RFC, כגון: O=, עבור Organization Name (שם ארגון) ו-C= עבור Country Name (שם ארץ) אינם משמשים בשירותי Active Directory, אף שהם מזוהים על ידי LDAP.

הערה לקריאת חומר נוסף אודות שמות ייחודיים, פנה לתקליטור המצורף לספר זה (\chapt06\articles\RFC1779.txt).

RDN - Relative Disinguished Name

בשירותי Active Directory ניתן לאתר אובייקט, אף אם אינך יודע בדיוק את השם הייחודי, במקרה שהשם הייחודי השתנה. זאת ניתן לעשות על ידי ביצוע שאילתה על מאפייני האובייקט. אחד ממאפייני האובייקט הוא RDN - **R**elative **D**istinguished **N**ame, שהוא חלק משם DN המלא. בדוגמה הקודמת, ה-RDN של האובייקט James Smith, הוא CN=James Smith. ה-RDN של אובייקט ההורה הוא CN=Users.

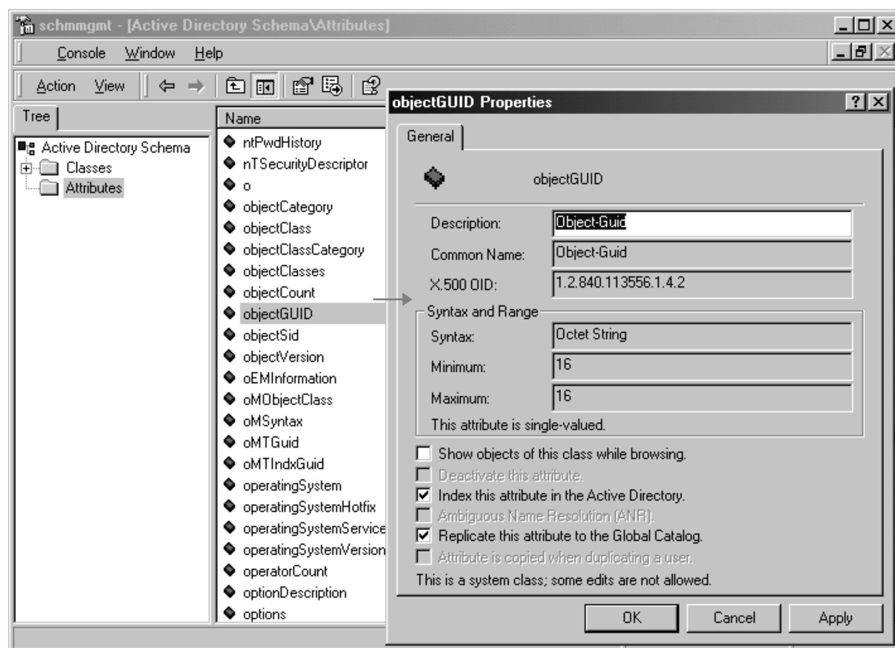
שירותי Active Directory מאפשרים RDN כפולים עבור אובייקטים, אך שני אובייקטים בעלי RDN זהה לא יכולים להתקיים בתוך OU אחת. לדוגמה, אם OU מכילה חשבון משתמש של James Smith, לא תוכל להוסיף משתמש נוסף בשם James Smith. אולם, אם ה-OU מכילה שתי OUs קטנות יותר, כגון מנהלים ומכירות, ב-OU של המנהלים יכול להיות חשבון משתמש בשם James Smith וב-OU של המכירות גם יכול להיות חשבון משתמש בשם James Smith, כיון שכל חשבון משתמש כזה יהיה בעל שם ייחודי (DN) שונה.

GUID - Globally Unique Identifier

בנוסף ל-DN, לכל אובייקט ב-Active Directory Store יש זיהוי ייחודי. ניתן להעביר אובייקטים ולשנות את שמם, אך זהותם לעולם לא משתנה. הזיהוי של אובייקט נקבע על ידי GUID - **G**lobally **U**nique **Id**entifier, מספר בן 128 סיביות המוקצה על ידי **D**irectory **S**ystem **A**gent (DSA, סוכן מערכת ספריית הרשת), כאשר האובייקט נוצר. שלא כמו שם ייחודי, או שם ייחודי יחסי, GUID לעולם אינו משתנה, אף אם תעביר או תשנה את שם האובייקט. יישומים יכולים לאחסן את GUID של אובייקט ולהיות בטוחים באחזור האובייקט ללא תלות ב-DN הנוכחי שלו.

במערכת Windows NT, ה-Domian Resources השתייכו ל- **S**ecurity **Id**entifier (SID, מזהה אבטחה), שנוצר בתוך ה-Domain. המשמעות היתה ש-SID היה ייחודי בתוך ה-domain. GUID הוא ייחודי לרוחב כל ה-Domains; תוכל להעביר אובייקטים מ-domain ל-domain, ועדיין יהיה להם מזהה ייחודי.

GUID מאוחסן במאפיין objectGUID, הקיים בכל אובייקט. המאפיין objectGUID מוגן, כך שלא ניתן לשנותו או להסירו. בעת אחסון הפניה לאובייקט Active Directory באחסון חיצוני (לדוגמה מסד נתונים של שרת SQL של Microsoft), יש להשתמש בערך objectGUID. תרשים 6.2 מפרט את התכונות של מאפיין objectGUID.



תרשים 6.2 מאפיין objectGUID כפי שהוא מופיע בתוסף התוכנה Active Directory Schema Management.

UPN - User Principal Name

UPN - **U**ser **P**rincipal **N**ame, הוא שם ידידותי, קצר יותר מ-DN וקל יותר לזכירה. UPN מורכב משם מקוצר (Shorthand) המייצג את המשתמש ואת שם DNS של ה-domain בו שוכן אובייקט המשתמש. פורמט UPN הוא שם המשתמש, עם תו "@", בתוספת סיומת של משתמש ידידותי. לדוגמה, המשתמש James Smith בעץ microsoft.com יכול להיות בעל UPN של username@microsoft. UPN אינו תלוי ב-DN של אובייקט המשתמש, כך שניתן להעביר או לשנות את האובייקט, מבלי להשפיע על שם ההתחברות. UPN הוא מאפיין (userPrincipalName) של אובייקט משתמש עיקרי (Security Principal Object).

הערה UPN מוכר לכולנו בהקשר ל- e-mail.

מבנה Active Directory

את מבנה Active Directory Services ניתן לפרק למספר מודלי ארכיטקטורה עיקריים:

- ❖ Data Model (מודל נתונים),
- ❖ Schema (סכמה),
- ❖ Security Model (מודל אבטחה),
- ❖ Administration Model (מודל ניהול).

Data Model

מודל הנתונים של Active Directory הוא נגזרת של מודל הנתונים X.500. ספריית הרשת מכילה אובייקטים המייצגים מספר רכיבים של הרשת, וכל אובייקט מתואר על ידי מאפיינים. אוסף האובייקטים שניתן לאחסן בספריית רשת מוגדרת בסכמה.

Schema

הסכמה (Schema) של Active Directory מיושמת כערכת מופעי מחלקת אובייקט המאוחסנת בספריית הרשת. ניתן לעדכן את הסכמה באופן דינמי. כלומר, יישום יכול להרחיב את הסכמה עם מאפיינים וסיווגים חדשים ויכול להשתמש בהרחבות מייד. עדכוני סכמה מבוצעים על ידי יצירה או שינוי של האובייקטים של הסכמה שמאוחסנים בספריית הרשת. כמו כל אובייקט ב-Active Directory, האובייקטים של הסכמה מוגנים על ידי רשימות בקרת גישה (**A**ccess **C**ontrol **L**ists - ACLs), כך שרק משתמשים מורשים (Authorized) יכולים לשנות את הסכמה.

Security Model

ספריית הרשת היא חלק מ-Trusted Computing Base של Windows 2000 והיא שותפה מלאה בתשתית האבטחה של Windows 2000. **Trusted Computing Base** הוא ערכת רכיבי מערכת ההפעלה האחראים על אכיפת מדיניות האבטחה של מערכת ההפעלה. ACLs מאבטחות את כל האובייקטים ב-Active Directory. שגרות אימות הגישה של Windows 2000 משתמשות ב-ACL לאימות כל ניסיון גישה לאובייקט או מאפיין ב-Active Directory.

Administration Model

משתמשים מורשים (Authorized) מבצעים פעולות ניהול בשירותי Active Directory. משתמש מקבל אישור מסמכות גבוהה יותר לביצוע פעולות מוגדרות על ערכת אירועי אובייקטים מוגדרת וסיווגי אובייקטים בתת עץ מזוהה כלשהו של ספריית הרשת. דבר זה נקרא ניהול מואצל (Delegated Administration). שיטה זו מאפשרת שליטה פרטנית על "מי יכול לעשות מה", ומאפשרת האצלת סמכויות ניהול ללא הענקת הרשאות עיליות.

DSA (סוכן מערכת ספריית הרשת) הוא ההליך שמנהל את האחסון הפיסי של ה-Directory (ספריית הרשת). לקוחות משתמשים באחד מהממשקים הנתמכים להתחבר ל-DSA ולחפש אובייקטים של ספריית הרשת לכתיבה וקריאה, ואת המאפיינים שלהם. DSA מאפשר בידוד הלקוח מפורמט האחסון הפיסי של נתוני ה-Directory. בכך מתאפשרת גישה נוחה ומשופרת לאבטחת המערכת.

גישה ל- Active Directory Services

הגישה ל-Active Directory Services היא באמצעות פרוטוקולי Wire. פרוטוקולים אלה מגדירים את פורמט ההודעות והתגובות של לקוח ושרת. מיגוון **A**pplication **P**rogramming **I**nterfaces (API, ממשקי פיתוח יישומים) מאפשרים גישה לפרוטוקולים אלה.

תמיכת פרוטוקול (Protocol Support)

מכלול Active Directory Services תומך בפרוטוקולים הבאים:

- **LDAP** – פרוטוקול הליבה של Active Directory הוא LDAP. LDAP בגירסאות 2 ו- 3 נתמכים.
- **MAPI-RPC** – מכלול Active Directory Services תומך בממשק **R**emote **P**rocedure **C**all (RPC, קריאה לשגרה מרוחקת) התומך בממשקי **M**essaging **A**pplication **P**rogram **I**nterface (MAPI, ממשק הודעות תוכניות יישומים).
- **X.500** – מודל הנתונים של Active Directory נגזר ממודל הנתונים X.500. X.500 מגדיר מספר פרוטוקולי Wire ששירותי Active Directory אינם מיישמים, חלקם, עקב תלותם בפרוטוקול רשת OSI:
  - **D**irectory **A**ccess **P**rotocol (DAP, פרוטוקול גישה ל-directory).
  - **D**irectory **S**ystem **P**rotocol (DSP, פרוטוקול מערכת directory).
  - **D**irectory **I**nformation **S**hadowing **P**rotocol (DISP, פרוטוקול מעקב נתוני ספריית הרשת).
  - **D**irectory **Op**erational Binding Management Control (DOP).

API - Application Programming Interfaces

שירותי Active Directory מספקים API - **A**pplication **P**rogramming **I**nterfaces חזקים, גמישים וקלים לשימוש. הזמינות של מיגוון עשיר של API עבור Active Directory, מעודדת פיתוח יישומים וכלים העושים שימוש בשירותי ספריית הרשת.

ADSI - Active Directory Services Interfaces

כדי להקל על כתיבת יישומים הניגשים ל-Active Directory Services ול-LDAP-Enabled directopry נוספים, Microsoft פיתחה את ADSI - **A**ctive **D**irectory **S**ervices **I**nterfaces. ADSI היא ערכת ממשקי תכנות ניתנת להרחבה וקלה לשימוש, המשמשת לכתיבת יישומים לגישה וניהול המשאבים הבאים:

- ❖ Active Directory Services.
- ❖ LDAP-Bases Directory
- ❖ שירותי ספריית רשת אחרים, כולל **N**ovell **D**irectory **S**ervice - NDS.

ADSI היא חלק מממשק ODSI - **O**pen **D**irectory **S**ervices **I**nterface, ו- WOSA - **W**indows **O**pen **S**ervices **A**rchitecture. אובייקטים של ADSI זמינים עבור Windows NT 4.0, Novell NetWare 3.x/4.x ו-Active Directory Services, בנוסף לכל Directory services התומך בפרוטוקול LDAP.

ADSI מחלצת את היכולות של directory Services מספקי רשתות שונים, כדי לספק ערכה בודדת של ממשקי directory services לניהול משאבי הרשת. דבר זה מפשט מאד פיתוח יישומים מבוזרים, כמו גם ניהול מערכות מבוזרות. מפתחים ו-Administrators משתמשים בערכה בודדת זו של Directory Services interfaces למספר ולנהל את המשאבים ב-Directory Service, בלי תלות בסביבת הרשת המכילה את המשאב. בכך, מקלה ADSI על ביצוע מטלות ניהול נפוצות, כמו הוספת משתמשים חדשים, ניהול מדפסות ואיתור משאבים בכל סביבת מערכת המחשוב המבוזרת. ADSI גם מקלה על מפתחים לגרום ליישומיהם להיות Directory-Enabled.

אובייקטים של ADSI מתוכננים להתאים לצרכי שלושת הגורמים העיקריים הבאים:

- ❖ **מפתחים** – ככלל, מפתחים ישתמשו ב-ADSI עם שפה מהודרת כגון C++, אף כי ניתן להשתמש בשפת Visual Basic לצורך בניית אב-טיפוס של היישום. לדוגמה, מפתח עשוי לכתוב יישום לניהול מספר ספריות רשת, רישות הדפסות, גיבוי מסדי נתונים וכדומה.
- ❖ **מנהלי מערכות** – ככלל, מנהלי מערכות יגשו ל- ADSI באמצעות שפת תסריט (Scripting Language) כגון Visual Basic, אף כי ניתן להשתמש ב-C\C++ לשיפור הביצועים. לדוגמה, עם Active Directory Services, יוכל Administrator לכתוב תסריט שיוסיף 100 משתמשים חדשים למערכת ולקבוע שהם יהיו חברים בקבוצות אבטחה נבחרות.
- ❖ **משתמשים** – כמו מנהלי מערכות, גם משתמשים יגשו ל-ADSI באמצעות שפת תסריט. לדוגמה, משתמש עשוי לכתוב תסריט לאיתור כל עבודות ההדפסה בקבוצה, או תורי הדפסה, ולהציג את המצב של כל אחד, במידה ויש את ההרשאות המתאימות.

LDAP C API

LDAP C API מספק את הפתרון בעל המכנה המשותף הנמוך ביותר, למפתחים שיישומיהם נדרשים לעבוד עם הרבה סוגים של לקוחות. בדומה, יישומי LDAP קיימים יפעלו עם Active Directory Services עם שינויים מעטים או ללא שינויים כלל, מעבר להרחבת היישום לתמיכה בסוגי אובייקטים הייחודיים ל- Active Directory Services. מומלץ למפתחים של יישומי LDAP לעבור ל-ADSI, התומכת בכל LDAP-Enabled directory services.

Windows Messaging API

מכלול Active Directory Services תומך ב- MAPI כך שיישומי MAPI מיושנים (Legacy) ימשיכו לעבוד עם Active Directory Services. אולם, מומלץ למפתחי יישומים חדשים לעבור ל-ADSI לבניית יישומים Directory-Enabled.

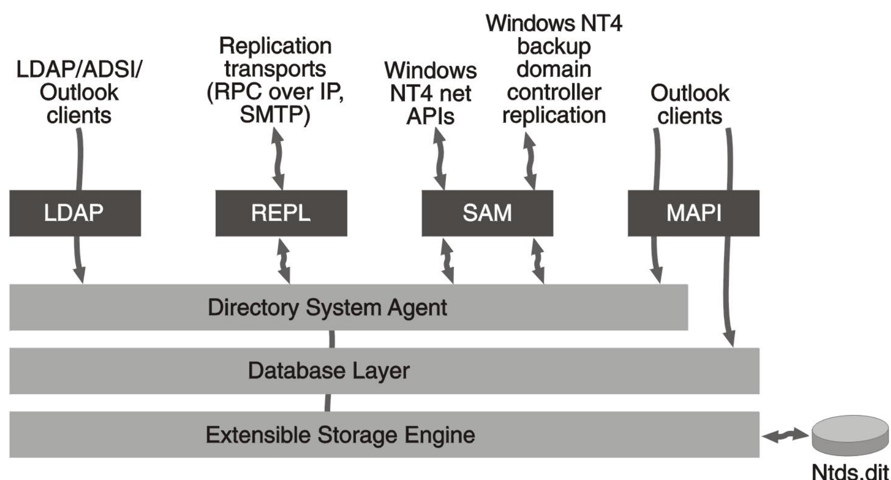
Virtual Containers

מכלול Active Directory Services תומך במכולות וירטואליות, המאפשרות גישה שקופה לכל directory תואם LDAP דרך Active Directory Services. המכולה הוירטואלית מיושמת דרך נתוני המיקום המאוחסנים ב-Active Directory. נתוני המיקום מתארים היכן ב-Active Directory צריך להופיע ה-Directory הזר, ושם ה-DNS של שרת השומר העתק של ה-Directory עצמו ואת ה-DN ממנו יש להתחיל את פעולות החיפוש ב-DS הזר.

Directory Srervices Architecture

ניתן להדגים את אופן תפקוד Active Directory כמבנה מרובד, בו השכבות מייצגות את ההליכים שבאמצעותם השרת מספק שירותי ספריית רשת ליישומי לקוחות (תרשים 6.3). מבנה Active Directory מורכב משלוש שכבות ומספר ממשקים ופרוטוקולים הפועלים יחדיו לאספקת Directory Services.

שלוש שכבות השירות - DSA, Database Layer (שכבת מסד הנתונים), ושכבת **E**xtensible **S**torage **E**ngine (ESE) שומרות את סוגי המידע השונים הנדרשים לאיתור רשומות במסד הנתונים של ה-Directory. מעל שכבות השירות במבנה זה נמצאים הפרוטוקולים וממשקי פיתוח היישומים (API) המאפשרים תקשורת בין לקוחות וה-Directory Services.



תרשים 6.3 מבנה Active Directory Services.

מבנה Active Directory Services כולל את שלושת מרכיבי המפתח הבאים:

- **Directory System Agent** (DSA) – בונה היררכיה מיחסי parent-child המאוחסנים בספריית הרשת. מספק ממשק פיתוח יישומים (API) לקריאות מכתובות בספריית הרשת.
- **Database Layer** – מספקת שכבת הפשטה (שכבה מוסתרת) בין היישומים ומסד הנתונים. קריאות ליישום לעולם אינן מבוצעות באופן ישיר למסד הנתונים; הן מנותבות דרך שכבת מסד הנתונים.
- **Extensible Storage Engine** (ESE) – מתקשר ישירות עם רשומות בודדות ב-directory store בהתבסס על מאפיין RDN של האובייקט.
- **Data Store** (קובץ הנתונים Ntds.dit) – קובץ זה מופעל רק על ידי Extensible Storage Engine (ESE). ניתן לנהל את הקובץ באמצעות כלי Ntdsutil.

הערה Ntdsutil.exe מותקן ב- %systemroot%\system32 בעת התקנת Windows 2000 Server.

הממשקים

לקוחות ניגשים לשירותי Active Directory באמצעות מנגנונים הנתמכים על ידי DSA. בטבלה להלן יש תיאור של כל מנגנון כזה:

ממשק	תיאור
LDAP	מספק API (ממשק פתוח יישומים) ללקוחות LDAP וחושף את ADSI כך שניתן לכתוב יישומים נוספים המסוגלים לתקשר עם Active Directory Services. לקוחות התומכים ב-LDAP משתמשים בו כדי להתחבר ל-Directory System Agent. Active Directory Services תומך ב-LDAP בגרסאות 2 ו- 3. לקוחות Windows 2000, כמו גם לקוחות Windows 9X שמותקנים אצלם רכיבי לקוח של Active Directory, משתמשים ב-LDAP גירסה 3 להתחבר ל-DSA. ADSI מהווה אמצעי להפשטת (הסתרת) ה-API של LDAP; אולם, רק LDAP משמש בשירותי Active Directory.
REPL	משמש את שירות השכפול ומסייע לשכפול Active Directory באמצעות RPC על IP (RPC over IP) או Simple Mail Transport Protocol - SMTP, המהווה חלק מערכת הפרוטוקולים TCP/IP. ניתן להשתמש ב-SMTP עבור שכפול בין אתרים בלבד; שכפול RPC על IP משמש לשכפול גם בין אתרים וגם בתוך אתר.
SAM	מספק תאימות של הרמות הנמוכות לסייע בתקשורת בין Domains של Windows 2000 ו-Windows NT. לקוחות Windows המשתמשים ב-Windows NT או מערכת מוקדמת יותר משתמשים בממשק SAM להתחבר ל-DSA. גם שכפול מ-Backup DCs במצב מעורב (Mixed Mode) עובר דרך ממשק SAM.
MAPI	לקוחות MAPI מיושנים, כגון לקוחות Microsoft Outlook Messaging and Collaboration, מתחברים ל-DSA באמצעות ממשק ספר כתובות MAPI RPC.

DSA - Directory System Agent

Directory **S**ystem **A**gent - DSA הוא ההליך של Active Directory, הפועל על כל DC ומנהל את כל פעילויות Directory Servicdes. הליך זה מנהל את האחסון הפיסי של ספריית הרשת. לקוחות משתמשים באחד הממשקים הנתמכים להתחבר ל-DSA, ואז לחפש אובייקטים של קריאה וכתיבה בספריית הרשת ואת מאפייניהם. DSA מבודד את הלקוח מפורמט האחסון הפיסי של נתוני ה-Directory.

DSA מספק גישה למחסן, שהוא קובץ מסד הנתונים המכיל מידע על ספריית הרשת הנמצא על הדיסק הקשיח. DSA הוא מושג X.500 המתאר את ההליך מצד-השרת היוצר מופע של שירות ספריית הרשת, כלומר כריכת יישומים ל-DSA.

DSA כולל ממשקים התומכים בסדרת פעילויות הליבה המוצגות להלן:

Object Identification

לכל אובייקט ב-Active Directory יש GUID קבוע המשויך לשם האובייקט במבנה מחרוזת. שם האובייקט אינו קבוע; ניתן לשנותו. כל ההתייחסויות הקבועות לאובייקט נשמרות במונחי GUID; שם האובייקט משמש לניווט בהיררכיה ולתצוגה. DSA שומר על שיוך ה-GUID לאובייקט כאשר ה-DN של האובייקט משתנה.

Transaction Processing

תנועות מעובדות באופן אוטומטי. בקשת כתיבה או שמתבצעת, ואז כל השפעותיה בנות-קיימא, או שהיא נכשלת לפני השלמתה, ואז אין לה כל השפעה. תנועות נכתבות בו-זמנית בקובץ יומן הפעולות (Transaction log file) ובמסד הנתונים.

Schema Enforcement of Updates

שיכפול וסנכרון נתוני ספריית הרשת ידוע כ- **Multimaster Replication** (שכפול מרובה מאסטרים). במערכת בה מאסטרים רבים, שינוי באובייקט סכמה בהעתק אחד, עלול להתנגש עם אובייקטים קיימים בהעתק זה וגם באובייקטים בהעתקים אחרים. הסכמה היא הגדרה רשמית של כל סיווג (Class) של אובייקט שניתן ליצור בספריית הרשת, המאפיינים של כל סיווג אובייקט, וההורים שיכולים להיות לכל סיווג אובייקט. במערכת Windows 2000 שינוי סכמה הוא **Single-Master Operation** (פעולה המבוצעת בידי מאסטר אחד), כלומר, כל שינוי שתבצע במאסטר יעודכן בכל שאר ההעתקים. עדכונים משוכפלים אינם מבצעים בדיקות סכמה. יצירת אחידות ועקביות בין האובייקטים המשוכפלים היא המטרה העיקרית; שמירה על אחידותם עם סכמה משתנה היא מטרה משנית.

Access Control Enforcement

DSA אוכף מגבלות אבטחה ב-Directory. שכבת DSA קוראת SID (זיהוי אבטחה) על אסימון הגישה.

Support for Replication

DSA מכיל Hooks (תפסים) עבור הודעות השכפול. כל עדכוני האובייקטים חייבים בסופו של דבר לעבור דרך הפעילות המתאימה כדי ששירות ספריית הרשת יפעל כנדרש.

Referrals

שכבת DSA מנהלת את נתוני היררכיית ה-Directory, המתקבלים משכבת מסד הנתונים. DSA אחראית להצלבת הפניות אובייקטים של Active Directory Domain במעלה ובמורד ההיררכיה, וגם החוצה להיררכיות Domain אחרות.

Database Layer

שכבת מסד הנתונים (Database Layer) מספקת נקודת מבט של אובייקט על נתוני מסד הנתונים, על ידי החלת סמנטיקת סכמה לרשומות במסד הנתונים, ובכך מבודדת את השכבות העליונות של שירות ה-directory מתשתית מערכת מסד הנתונים. שכבת מסד הנתונים היא ממשק פנימי שאינו חשוף. שום קריאה למסד הנתונים אינה מתבצעת באופן ישיר ל- **E**xtensible **S**torage **E**ngine (ESE); במקום זאת, כל גישה למסד הנתונים מנותבת דרך שכבת מסד הנתונים.

מכלול Active Directory Services נותן Namespace היררכי. כל אובייקט מזוהה ייחודית במסד הנתונים באמצעות מאפיין השם הייחודי שלו, הנקרא RDN. RDN וסדרת שמות הורי האובייקט מהווים את השם הייחודי של האובייקט. מסד הנתונים אוגר את ה-RDN עבור כל אובייקט כמו גם הפניה לאובייקט ההורה. שכבת מסד הנתונים עוקבת אחר הפניות הורים אלו, ומרכזת את סדרת ה-RDN ליצירת שם ייחודי.

פעולה מרכזית של שכבת מסד הנתונים היא לתרגם כל DN למבנה Integer (מספר שלם) הנקרא DN tag, המשמש לכל הגישות הפנימיות. שכבת מסד הנתונים מבטיחה שכל DN tag יהיה ייחודי עבור כל רשומה במסד הנתונים.

כל נתון המתאר אובייקט מוחזק כערכת מאפיינים, המאוחסנת כעמודה במסד הנתונים. שכבת מסד הנתונים אחראית ליצירה, אחזור ומחיקת רשומות בודדות, מאפיינים עם רשומות וערכים בתוך מאפיינים. לביצוע מטלות אלו, שכבת מסד הנתונים משתמשת בזיכרון המטמון של הסכמה (מבנה בתוך-הזיכרון ב-DSA) לקבלת מידע אודות המאפיינים הדרושים לה.

ESE - Extensible Storage Engine

מכלול Active Directory Services מיושם על גבי **I**ndexed **S**equential **A**ccess **M**ethod (ISAM, שיטת גישה באמצעות אינדקס רציף). גירסה קודמת של מנהל טבלה זה, הנקראת בשם Jet database, משמשת במערכת Microsoft Exchange Server גירסה 5.5, File Replication Service, בעריכת תצורת אבטחה, בשרת האישורים, בשירות למתן שמות אינטרנט של Windows (WINS), ובמספר רכיבי Windows נוספים. למערכת Windows 2000 יש גירסה חדשה ומשופרת של מסד הנתונים JET, בשם ESE - **E**xtensible **S**torage **E**ngine.

ESE (Esent.dll) מיישם מערכת מסד נתוני המשתמשת בקובץ יומן כדי לוודא שהתנועות המבוצעות אכן בטוחות. מכאן, ששירותי ספריית הרשת משתמשים גם

בקבצי נתונים (Ntds.dit) ובקבצי יומן. מיקום ברירת המחדל של הקבצים Ntds.dit ו-Esent.dll הוא בתיקיה systemroot%\system32%.

ESE אוגר את כל האובייקטים של Active Directory. ESE תומך במסד נתונים בגודל של עד 16TB, אשר תיאורטית, יכול לשמור מיליונים רבים של אובייקטים בכל Domain.

ESE מתאים מאוד לצרכי אחסון ב-Active Directory Services:

- ❖ פעולות עדכון של ESE מבוצעות ליצירת יציבות ושלמות, למקרה של כשלים במערכת.
- ❖ ESE מטפלת היטב בשורות נתונים דלילות (Sparse rows), כלומר בשורות בהן למאפיינים רבים אין ערכים.

מכלול Active Directory Services מגיע עם סכמה מוגדרת מראש, המגדירה את כל המאפיינים הדרושים והמותרים עבור אובייקט נתון. ESE מקצה שטח אחסון רק עבור השטח הנצרך - כלומר רק למאפיינים המוקצים לאובייקט, לא עבור כל המאפיינים האפשריים. לדוגמה, אם לאובייקט של משתמש יש כבר 50 מאפיינים המוגדרים בסכמה, ואתה יוצר משתמש עם ארבעה מאפיינים בלבד, שטח אחסון מוקצה רק עבור ארבעה מאפיינים אלה. אם מתווספים מאפיינים נוספים מאוחר יותר, מוקצה להם שטח אחסון נוסף.

כמו כן, ESE מסוגל לאגור מאפיינים בעלי ערכים רבים. לדוגמה, מסד הנתונים יכול לאחסן מספרי טלפון רבים עבור משתמש בודד, מבלי לדרוש מאפיין מספר טלפון שונה עבור כל מספר טלפון.

מכלול Active Directory Services הוא ערכה תפקודית מוגברת של Exchange Server Directory Services; הוא מציע תפקודיות מורחבת, כגון אובייקטים בטוחים מפני שינוי שמות, סכמה מתרחבת דינמית ושכפול לפי מאפיין ולפי השלמה. קובץ Esent.dll מיישם את תפקודיות החיפוש והאחזור של מסד הנתונים.

סיכום שיעור

מכלול Active Directory Services מהווה סביבת עבודה היררכית, הניתנת להרחבה והגדלה ובעלת אבטחה מבוזרת הנדרשת על ידי לקוחות עסקיים. הוא משלב את מושג NameSpace של האינטרנט עם Directory Services של מערכת ההפעלה. הוא משתמש ב-LDAP כפרוטוקול הליבה שלו ומסוגל לעבוד מעבר לגבולות מערכת ההפעלה, ובכך לחבר Namespaces רבים. הסכמה של Active Directory כוללת הגדרה רשמית של תכולת Active Directory store ומבנהו, כולל כל המאפיינים, הסיווגים ומאפייני הסיווגים. ה-Global Catalog, שהוא מקום המידע המרכזי אודות אובייקטים בעץ או ביער, הוא נקודת שירות ואחסון פיסי המכיל העתק של מאפיינים נבחרים של כל אובייקט ב-Active Directory store. כמו כל Directory Services, מכלול Active Directory Services הוא בעיקרו Namespace, וכל אובייקט ב-Active Directory מזוהה עם שם. מבנה Active Directory Services ניתן לפירוק למספר רכיבי מבנה עיקריים: מודל הנתונים, סכמה, מודל האבטחה ומודל הניהול. גישה לשירותי Active Directory היא באמצעות פרוטוקולים המגדירים את פורמט ההודעות ותעבורת לקוח ושרת. מבנה Active Directory מורכב משלוש שכבות שירות ומספר ממשקים ופרוטוקולים הפועלים יחד לאספקת שירותי ספריית רשת.

שיעור 2: תכנון יישום Active Directory

לפני יישום סביבת רשת Windows 2000, עליך לשקול תחילה כיצד ליישם את Active Directory Services. קח בחשבון את המבנה העסקי והתפעולי של הארגון אליו אתה שייך, כגון המיקום הפיסי של המשרדים, גידול וארגון מחדש עתידיים וגישה למשאבי הרשת. קיימים מספר היבטים של יישום Active Directory המהווים חלק מתהליך התכנון. תחילה עליך לתכנן את DNS Namespace (**D**omain **N**ame **S**ystem). ה-Namespace כולל את היררכיית ה-Domain, את ה-Global Catalog, את Trust Relationship (יחסי האמון) ואת ה-Replication (שכפול). בנוסף, Namespace כולל גם OU, שיש לקחת בחשבון בהליך התכנון. ב-Domain בודד, ניתן לארגן משתמשים ומשאבים על ידי שימוש בהיררכיית OUs המשקפת את מבנה החברה. לבסוף, הליך התכנון לקראת יישום Active Directory, חייב לכלול תוכנית לייסוד אתרים שיכולים לסייע ביעילות לתהליך ניהול השכפול ותעבורת ההתחברות על פני קישורים בארגון.

לאחר שיעור זה, תוכל

- **לתכנן** Namespace, Site **ו-**OUs , כהכנה **ליישום** Active Directory.

זמן לימוד משוער: 75 דקות

תכנון Namespace

בדומה ל-DNS, Namespace של Active Directory הוא Domain Name ברמה הגבוהה ביותר ובעל יכולות מלאות עבור חברה המורכבת מ- Windows 2000 Domains, DCs, OUs, יחסי אמון ו- Domain Trees. אחת ההחלטות, שעליך לקבל בעת יישום Active Directory Services, היא אם ה-Namespace הפנימי (בתוך ה-Firewall, קיר מגן), וה-Namespace החיצוני (מחוץ ל- Firewall) יהיו זהים, או נפרדים. במילים פשוטות, האם ה-Namespace של ה- Active Directory יתאים ל-Namespace של ה- DNS (בדרך כלל שם Domain האינטרנט האופייני), שעלול להיות מוגדר כבר עבור החברה שלך?

לדוגמה, DNS Namespace החיצוני הקיים עשוי להיות microsoft.com. תוכל לבחור Active Directory Namespace התואם ל-microsoft.com, או תוכל לבחור Namespace פנימי אחר. לכל אחד יש יתרונות וחסרונות כפי שיוסבר בהמשך פרק זה.

הערה מכאן לא נובע ש-DNS הוא Namespace **חיצוני** בלבד. הנקודה היא, שאם ה-Namespaces נפרדים, **ינוהלו שירותי** Active Directory **בנפרד מה-Namespace החיצוני.**

Internal and External Namespaces

Namespace הוא השמות ברמה הגבוהה ביותר ל-Active Directoty Domain Name של ארגון. ליישום Active Directory Services, ישנן שתי אפשרויות ל-Namespaces (טווחי שמות). Active Directory Namespace יכול להיות זהה או שונה מ-DNS Namespace החיצוני והרשום בארגון השמות של האינטרנט.

הסעיפים הבאים מתארים שני תרחישים; האחד בו ה-Namespaces זהים, והשני בו הם שונים. בתרחיש הראשון, בו טווחי שמות החיצוניים והפנימיים זהים, אותו Domain ברמה העילית מופיע משני צדי ה-Firewall. משתמשים פרטיים של רשת החברה ומשתמשים ציבוריים של האינטרנט רואים את השם microsoft.com. בתרחיש השני, בו טווחי השמות החיצוניים והפנימיים שונים, שם ה-domain ברמה העילית שבתוך קיר המגן שונה מהשם הרשום של ה-DNS Domain Name ברמה העילית של ה- Domain הנצפה על ידי האינטרנט. טווח השמות הפנימי (Internal Namespace) הוא expedia.com, וטווח השמות החיצוני (External Namespace) הוא microsoft.com.

תרחיש 1: טווחי שמות פנימיים וחיצוניים זהים

בתרחיש זה, החברה משתמשת באותו שם עבור טווח השמות הפנימי והחיצוני. microsoft.com משמש בתוך ומחוץ לחברה. ליישום תרחיש זה יש לעמוד בדרישות הבאות:

- לקוחות ברשת הפנימית, הפרטית של החברה חייבים להיות בעלי יכולת גישה לשרתים פנימיים וחיצוניים (שני צידי ה-Firewall).
- לקוחות הניגשים למשאבים מבחוץ, אסור שתהיה להם אפשרות גישה למשאבי החברה הפנימיים, ואסור שיוכלו להסדיר שמות.

כדי שתרחיש זה יעבוד, חייבים להתקיים שני אזורי DNS נפרדים. אזור אחד יתקיים מחוץ לקיר המגן, ויספק הסדרת שמות למשאבים ציבוריים. אזור זה אינו מוגדר לספק הסדרת שמות למשאבים פנימיים, ובכך מונע גישה למשאבי החברה הפנימיים על ידי לקוחות חיצוניים.

האתגר בתצורה זו הוא לתת גישה ציבורית למשאבים הנגישים ללקוחות פנימיים, כיון שאזור DNS החיצוני לא מוגדר להסדיר שמות למשאבים פנימיים. פתרון אחד הוא שכפול האזור החיצוני על DNS פנימי כדי לתת פתרונות ללקוחות פנימיים. אם משתמשים ב-Proxy, יש להגדיר את לקוח ה- Proxy כך שיתייחס ל-microsoft.com כמשאב פנימי.

הכוונה בתרחיש זה היא שאנשים מבחוץ הגולשים לאתר האינטרנט של החברה לא יוכלו לגשת לרשת הפנימית שלה.

יתרונות

שימוש בטווח שמות פנימי וחיצוני זהה כולל את היתרונות הבאים:

- שם העץ, microsoft.com, אחיד ברשת הפנימית הפרטית, וכן ברשת האינטרנט הציבורית.
- תרחיש זה מרחיב את הרעיון של שם התחברות יחיד לאינטרנט הציבורי, בכך שהוא מאפשר למשתמשים להשתמש בשם התחברות זהה להתחברות למערכת הפנימית והחיצונית. לדוגמה, username@microsoft.com ישמש כשם התחברות וגם זיהוי דואר אלקטרוני.
- חסכון ברישום שמות ב-DNS של האינטרנט.

חסרונות

לשימוש בשם זהה עבור טווחי שמות פנימיים וחיצוניים גם חסרונות כדלקמן:

- ההגדרה מסובכת יותר. יש להגדיר לקוחות Proxy, כך שיבחינו בין משאבים פנימיים וחיצוניים.
- יש להקפיד שלא לפרסם משאבים פנימיים באינטרנט.
- יוצר כפל מאמץ בניהול משאבים. לדוגמה, תחזוקת רשומות אזור כפולות עבור הסדרת שמות פנימיים וחיצוניים.
- אף שטווח השמות זהה, המשתמשים יקבלו תצוגה שונה של משאבים פנימיים וחיצוניים.

תרחיש 2: טווחי שמות פנימיים וחיצוניים נפרדים

בתרחיש זה, החברה משתמשת בטווחי שמות פנימיים וחיצוניים נפרדים. כתוצאה מכך, השמות משני עברי ה-Firewall שונים. שמות נפרדים משמשים בתוך ומחוץ לחברה. microsoft.com הוא השם שמתגלה למשתמשי האינטרנט ובו הם משתמשים. expedia.com הוא השם שרואים משתמשי הרשת הפרטית, ובו הם משתמשים. מומלץ לרשום את שני טווחי השמות ב-DNS של האינטרנט. רישום כזה מונע את "תפישת" השם באינטרנט ורישומו על ידי ארגון אחר. אם השם הפנימי אינו שמור ומשמש ארגון אחר, לקוחות פנימיים אינם יכולים להבחין בין השם הפנימי וטווח שמות DNS הציבורי הרשום.

ייווצרו שני אזורים. אזור אחד ישתמש ב-microsoft.com והשני ישתמש ב-expedia.com. לקוחות יכולים להבחין בין משאבים פנימיים לחיצוניים באופן ברור.

יתרונות

שימוש בטווחי שמות פנימיים וחיצוניים נפרדים כולל את היתרונות הבאים :

- ❖ כאשר מתבססים על שמות תחומים שונים, ההבדל בין משאבים פנימיים וחיצוניים ברור.
- ❖ אין חפיפה או כפילות מאמצים, וכתוצאה מכך נוצרת סביבה קלה יותר לניהול.
- ❖ הגדרת לקוחות Proxy פשוטה יותר, כיון שרשימות אי-הכללה צריכות להכיל רק את expedia.com בעת זיהוי משאבים חיצוניים.

חסרונות

לשימוש בשם נפרד עבור טווח שמות פנימי וחיצוני ישנם החסרונות הבאים :

- ❖ שמות התחברות שונים משמות דואר אלקטרוני. לדוגמה, אם מישהו מתחבר עם username@microsoft.com, אך כתובת הדואר האלקטרוני שלו היא username@expedia.com, עליו לזכור ולתחזק שני שמות משתמש נפרדים.
- ❖ רישום השם הפנימי ב-DNS של האינטרנט, כדי למנוע מארגון אחר את השימוש הציבורי בו.

טיפ בתרחיש זה, שמות ההתחברות הם שונים כברירת מחדל. מנהל יכול להשתמש ב-**M**icrosoft **M**anagement **C**onsole (MMC) לשינוי תכונות של סיומת UPN של משתמשים, כך ששם ההתחברות של המשתמש יתאים לכתובת הדואר האלקטרוני שלו.

Defining a Namespace Architecture

בנוסף להחלטה אם להשתמש ב-Namespaces (טווחי שמות) חיצוניים ופנימיים שונים או זהים, משתנים נוספים ישפיעו על מבנה טווח השמות. שיקול עיקרי הוא השפעת תעבורת השכפול ברשתות מרחביות (WAN). בנוסף, ארגונים והמבנה שלהם משתנים בקביעות. פרט ליכולת ליצור Windows 2000 forest, מנהלי רשתות (Administrators) צריכים להיות מסוגלים גם לשנות את מבנה טווח השמות ללא הוצאה גדולה ותוך הפרעה מזערית ככל שניתן. המטרה היא ליצור מבנה טווח שמות הניתן להגדלה, בעל יכולת הסתגלות לשינויים, יכולת הבחנה בין משאבים חיצוניים למשאבים פנימיים ויכולת להגן על נתוני החברה באותו זמן.

מבנה טווח שמות צריך לייצג את מבנה החברה, אך באותו זמן חייב לספק את הניהול הפרטני, הנדרש לניהול רשת גלובלית על פני הארגון כולו, המבוססת על Active Directory Services. בנוסף, המבנה חייב להיות בעל יכולת הרחבה וגידול, כדי לתמוך בשינויים ארגוניים ושינויים שדורשת ההנהלה.

דרך אחת לבצע זאת היא באמצעות שלוש שכבות תחומים :

- ❖ Root Domain
- ❖ First-layer Domain
- ❖ Second-layer Domain

מבנה זה מאפשר טופולוגיית שכפול פרטנית, ויכולת להגביל את מרחב ה-Administrators כנדרש.

Root Domain

Root Domain הוא ה- Domain הראשון ב-Namespace (טווח שמות), כגון expedia.com. Root Domain ב-Active Directory Services ממופה לטווח השמות של החברה. כל התחומים הפנימיים הם חלק מ-Domain זה, ובכך יוצרים טווח שמות רציף, מחובר בצורת Domain tree. בנוסף, שרתים המכילים את Namespace Root לא יתקיימו בצד הציבורי של ה-Firewall ולכן לא יהיו גלויים לאינטרנט.

First-Layer Domains

מטרת שכבה זו במודל היא יצירת Domain Names שאינם משתנים, גם אם אירעו שינויים בארגון הפנימי של החברה. הדרך הטובה ביותר לעשות זאת, היא על ידי מתן שמות ל-Domains ברמה זו בהתבסס על גבולות יבשתיים, גיאוגרפיים, או פוליטיים, לדוגמה, noamer.expedia.com או europe.microsoft.com. בנוסף, הדבר יסייע לצמצם שכפול שירות ישיר, כיון שמשתמש בצפון אמריקה אינו חייב להתקיים בשרתי Active Directory Services של שרת הממוקם באירופה. אולם, שרתי קטלוג גלובלי עדיין מאפשרים למשתמש בצפון אמריקה למצוא משאב באירופה כנדרש.

יחסי האמון (Trust Relationships) בין השורש וכל תחומי ה-First-layer Domains מאפשרים זמינות משאבים לכל הענפים של Domain tree. אי לכך, משתמש הנמצא ב-noamer.expedia.com יכול לגשת למשאב הנמצא ב-europe.microsoft.com.

Domain Names בשכבה זו חייבים להיות בני שלושה תווים לפחות, כדי שלא יתנגשו עם תקן ISO 3166. תקן זה מחייב שני תווים עבור קוד המדינה ב-Second-layer Domains וב-OUs.

הערה לסקירה על קוד שתי-אותיות לזיהוי ארצות לפי תקן ISO 3166, פנה לתקליטור המצורף לספר זה (\chapt06\articles\iso3166.txt). למידע עדכני ביותר על קודים של ארצות, גש למנוע חיפוש באינטרנט וחפש לפי מילות המפתח: ISO3166 או ISO+3166.

ההנחה היא שה-First-layer Domain יציבה ואינה משתנה.

הטבלה הבאה מהווה רשימת הצעות של מוסכמות למתן שמות:

domain	**הגדרה**
CORPIT	מטה ראשי של תחום טכנולוגיות המידע בחברה
NOAMER	ארצות הברית וקנדה
SOAMER	מקסיקו, מרכז אמריקה ודרום אמריקה
NOPAC	הונג-קונג ואתרים צפונית להונג-קונג (יפן, קוריאה, סין, טייוואן)
SOPAC	אתרים דרומית להונג-קונג, כולל תת היבשת ההודית עד, אך לא כולל אפגאניסטאן
EUROPE	אוסטריה, בלגיה, שוויץ, הרפובליקה הצ׳כית, דנמרק, ספרד, פינלנד, יוון, קרואטיה, הונגריה, אירלנד, איטליה, הולנד, נורווגיה, פולין, פורטוגל, רומניה, רוסיה, שוודיה, סלובקיה, סלובניה
MEAST	איחוד האמירויות הערביות, ישראל, ערב הסעודית, טורקיה
AFRICA	אפריקה
PARTNERS	שותפים עסקיים וחברות שמוציאים אליהם עבודות
JVT	מיזמים משותפים

חשוב מוסכמות אלו למתן שמות הן הצעות בלבד, שאינן סותרות את תקן ISO 3166 למתן שמות. ארגונים יכולים לבחור כל שיטה למתן שמות המתאימה למדיניותם ולצרכיהם.

Second-layer Domains

במצב אידיאלי, Domains בשכבה זו צריכים להיות ארצות בלבד, ולהוות ענף מה-Domains המקבילים שבשכבה הראשונה. היתרון בשיטה זו הוא שניתן ליצור Child-level domains מתחת ל-Second-layer Domains.

השתמש באותן מוסכמות למתן שמות בעת יצירת יחידות ארגוניות (OU) ב-Domain. כך מתאפשר קידום יחידה ארגונית ל-Domain, אם נדרש, עם השפעה מזערית על המשתמש.

בעת מתן שמות לאתרים בתוך ארה״ב, **אין** להשתמש בסטנדרט ISO 3166. במקום זאת, השתמש במיקוד דואר בן שתי ספרות לשמות מקומות. היוצא מהכלל היחיד להוראה זו היא קליפורניה, המתנגשת עם קוד ISO לקנדה. השתמש ב-CALIF בעת יצירת תחומים עבור קליפורניה.

לדוגמה, usa.noamer.microsoft.com הוא Second-layer domain, ואילו ny.usa.noamer.microsoft.com הוא Child-level domain.

Planning Organizational Units (OUs)

Organizational **U**nits - OUs צריכות לשקף את פרטי המבנה העסקי של החברה. צור OUs (יחידות ארגוניות) להאצלת סמכויות ניהוליות על קבוצות משתמשים קטנות, קבוצות ומשאבים. הסמכות הניהולית המואצלת יכולה להיות מלאה (יצירת משתמשים, שינוי סיסמאות, ניהול מדיניות חשבונות וכו'), או מוגבלת (מוגבלת אפילו עד סמכות טיפול בתור להדפסות בלבד). כיון ש-OUs ברמת-על יכולות לשמור רמות נוספות של OUs, ניתן להרחיב את רמת הפירוט כנדרש. ארגן אובייקטים אלה במבנה לוגי, מפה את אופן עבודתך וארגון עסקיך.

OUs מונעות את הצורך להעניק למשתמשים גישה ניהולית ברמת ה-Domain לביצוע מטלות כמו יצירת חשבונות מחשב והגדרת סיסמאות. ניתן עתה לתת למשתמשים Administrative control ברמת ה-OU, ובכך לשחרר Domain administrators ממטלות אלה. יחידות ארגוניות מוסיפות רמת אבטחה נוספת, בכך שהן מאפשרות ראות מוגבלת (באמצעות שימוש ב- ACL - רשימות בקרת גישה) של משאבים; משתמשים יכולים לראות רק אובייקטים שאליהם אושרה גישתם.

OUs יורשות את מדיניות האבטחה של ה-Parent domain וה-OU parent, אלא אם כן בוטלו בכוונה.

יצירת OU Structure

רצוי להתחיל תכנון OU (יחידה ארגונית) על ידי יצירת יחידה ארגונית ל-Domain הראשון ב-Namespace. השתמש ב-Domain וב-OU Structure כמודל לכל Domain המתוסף לעסק. בנוסף, מבנה היחידה הארגונית שנוצר צריך לתמוך במבנה עתידי, תוך תזוזת אובייקטים מזערית.

בכל פעם שיחידה ארגונית נוצרת, חשוב לקבוע מי יוכל לעיין ולשלוט באובייקטים מסוימים, ואיזו רמת Administration תהיה לכל Administrator על האובייקטים. בנוסף, נדרש לקבוע לאיזה Administrators תהיה זכות גלובלית ליחידות ארגוניות ואובייקטים מסוימים, איזה Administrators יהיו מוגבלים, ומה תהיה רמת הגבלה זו.

OU Design Guidelines

השתמש בהנחיות הבאות ליצירת OUs (יחידות ארגוניות):

- צור יחידות ארגוניות להאצלת סמכויות administration.
- צור מבנה יחידות ארגוניות הגיוני ובעל משמעות, המאפשר ל-OU administartors לבצע את המטלות שלהם ביעילות.
- צור יחידות ארגוניות ליישום מדיניות אבטחה.
- צור יחידות ארגוניות כדי לאפשר או להגביל עיון במשאבים שנוצרו על ידי משתמשים מסוימים.
- צור תשתית יציבה יחסית של יחידות ארגוניות. היחידות הארגוניות גם יוצרות גמישות של Namespace (טווח שמות), כדי להתאים לצרכיו המשתנים של העסק.
- הימנע מהקצאת child-objects רבים מדי לכל אחת מה-OUs.

כאשר תתחיל לתכנן מבנה יחידה ארגונית, זכור לתת שמות בעלי מבנה היררכי, אחיד ויציב, וכלליים דיים לשימוש בכל Domain בארגון ליחידות הארגוניות ולאובייקטים. נסה להימנע מכך שליחידה ארגונית יהיו child-objects רבים מדי, מכיון שהם עלולים ליצור צווארי בקבוק בעת ביצוע חיפושים ושאילתות ניווט.

שיטה אחת, ליצירת מבנה יחידה ארגונית עבור ה-domain הראשון, היא לתת ליחידות הארגוניות ברמות העליונות שם אשר הופך לכותרות. כותרות אלו מגדירות את היחידות הארגוניות המפורטות יותר ואת האובייקטים שמתחת להן. גישה אחרת ליצירת מבנה יחידות ארגוניות אחיד היא להתחיל בקביעת ההיררכיה הטבעית של האובייקטים. לאחר שמיינת את האובייקטים הבודדים באופן היררכי לקבוצות, ניתן לתייג אותם עם שמות יחידות ארגוניות ברמה העליונה.

אם יש Multiple domains בתכנון, קבע אם ניתן להשתמש במבנה היחידות הארגוניות על פני כל ה-Domains. אם לא, חזור ותכנן מחדש.

Structure the OU Hierarchy

חשוב ביותר לקבוע מה התפיסה שתשמש כבסיס ל- OU Hierarchy (היררכיית היחידה הארגונית). חברות רבות מבססות את מבנה ה-Domain שלהן על מודל המשקף את מבנה עסקיהן. הסיווגים הבאים הם דרכים שונות לסיווג היררכיית היחידות הארגוניות.

Administration or Object-Based OUs

כאשר מבנה היחידה הארגונית מבוסס על administrative model, כל ה-administrators בעלי היחידה הארגונית יוצאים נשכרים. בשירותי Active Directory ניתן ליצור יחידות ארגוניות המבוססות על אובייקטים, כגון משתמשים, מחשבים, יישומים, קבוצות, מדפסות, מדיניות אבטחה ועוד. כאשר Administration-based OUs נוצרות בצורה הגיונית ובעלת משמעות, הדבר מסייע ל-Administrators לבצע את עבודתם במהירות ובקלות. ברוב המקרים, זו הדרך הטובה ביותר לארגן יחידות ארגוניות, כיון שבכך יובטח מספר השינויים הקטן ביותר.

Geographical-Based OUs

ניתן ליצור יחידות ארגוניות המכילות את כל הפעילות העסקית בכל אתר גיאוגרפי. שוב, גם מבנה זה יהיה יציב לאורך זמן. אולם, אם צפויים שינויים גדולים במבנה הארגוני של החברה, שקול בסיס אחר לתכנון היחידות הארגוניות.

Business Function-Based OUs

אם יש הגיון בכך, ניתן ליצור יחידות ארגוניות המבוססות על תפקודים עסקיים שונים בתוך החברה, כגון שווק, IT (טכנולוגיות מידע), כספרים ותפעול. תפקודים אלה עשויים להיות יציבים אף אם הארגון הייחודי שמבצע אותם אינו יציב.

Department-Based OUs

גישה נוספת היא יצירת יחידות ארגוניות המשקפות את הקשר ל-Cost center. שיטה זו תמפה את הארגון הנוכחי, אך תהיה לה נטייה להיות בלתי יציבה ככל שהעסק עובר שינויים מבניים.

Project-Based OUs

השתמש במודל יחידה ארגונית זה לשייך Cost center עם פרויקט, ולא עם מחלקה. יש חברות שעסקיהן מונעים על ידי פרויקטים; לדוגמה, פיתוח תוכנה, תעשיית התעופה ועוד. זו הסיבה שחברה תרצה ליצור יחידות ארגוניות מבוססות-פרוייקטים. מבנה יחידה ארגונית זו אינו מומלץ, שכן הוא אינו נחשב ליציב. ככלל, סוג זה של יחידה ארגונית יהיה child של יחידה ארגונית יציבה יותר. זכור לקבוע מי ינהל (Administrator) יחידה ארגונית זו.

Planning a Site

עד לנקודה זו בשיעור, דנו במבנה הלוגי של Domains ו-OUs. תשומת לב לתכנון הפיסי גם היא קריטית ליישום מוצלח של רשת Windows 2000 Server התומכת ב-Active Directory Services. המבנה הפיסי של רשת מבוססת Windows 2000 Server מתבטא באתר. אתר (Site) הוא שילוב של IP Subnet אחת או יותר המחוברות בקישורים מהירים. לעיתים קרובות לאתר יש גבולות זהים לרשת מקומית (LAN) או רשת המרחבית (WAN) בעלת רוחב פס גבוה ביותר כגון OC3 SONET (155Mbps) או T3 WAN (45Mbps).

מנוע השכפול של Active Directory מאפשר הבחנה בין שכפול המתרחש בחיבור לרשת מקומית, ושכפול המתרחש בחיבור ברשת מרחבית (WAN) בעלת רוחב פס נמוך. תעבורת הרשת באתר תהיה בדרך כלל גבוהה יותר מתעבורה בין אתרים.

אופן הגדרת האתרים משפיע על Windows 2000 בשתי דרכים:

- ❖ **Workstation Logon** (התחברות תחנת עבודה) – כאשר משתמש מתחבר, לקוחות בעלי הרשאות Active Directory Services ינסו לאתר DC באותו Site בו מותקן מחשב המשתמש, כדי לשרת את בקשת ההתחברות שלו ובקשות נוספות לנתונים מהרשת.
- ❖ **Directory Replication** (שכפול ספריית הרשת) – ניתן להגדיר את התזמון ונתיב השכפול של ספריית הרשת של ה-Domain באופן אחד עבור שכפול בין אתרים, ובאופן שונה לשכפול בתוך האתר. ככלל, שכפול בין אתרים נוטה להיות פחות תכוף משכפול בתוך אתר.

בשירותי Active Directory, אתרים אינם חלק מטווח השמות. בעת דפדוף בטווח שמות לוגי, תראה משתמשים ומחשבים המקובצים ב-Domains וב-OUs - לא ב-Sites. מבנה האתר (Site) נשמר בחלק נפרד של ה-Directory. אתרים מכילים רק אובייקטים של מחשבים ואובייקטים של חיבורים המשמשים להגדרת שכפול בין אתרים.

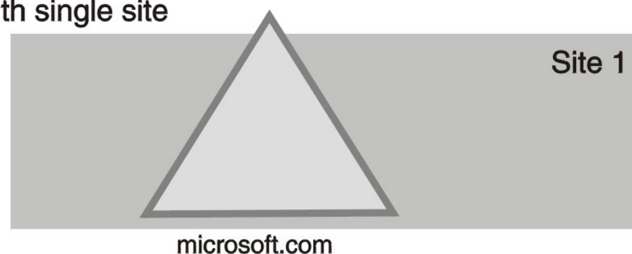
אתרים מתוכננים כראוי מבטיחים שקישורי רשתות לא יגיעו לרוויה כתוצאה מתעבורת שכפול, ששירותי Active Directory יישארו עדכניים, ושמחשבי לקוחות יגשו למשאבים הקרובים אליהם ביותר.

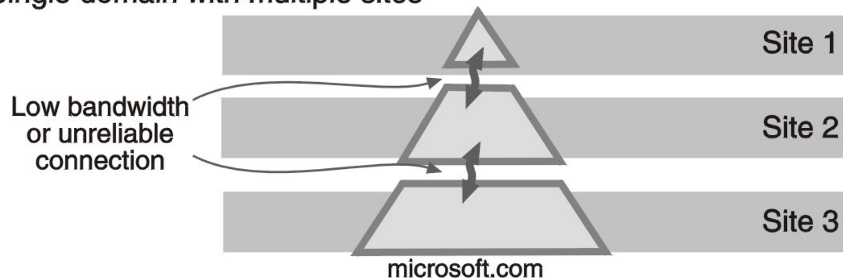
בעת תכנון אופן קיבוץ Subnets (תת-רשתות) ליצירת Sites (אתרים), שקול את מהירות התעבורה בין תת-הרשתות.

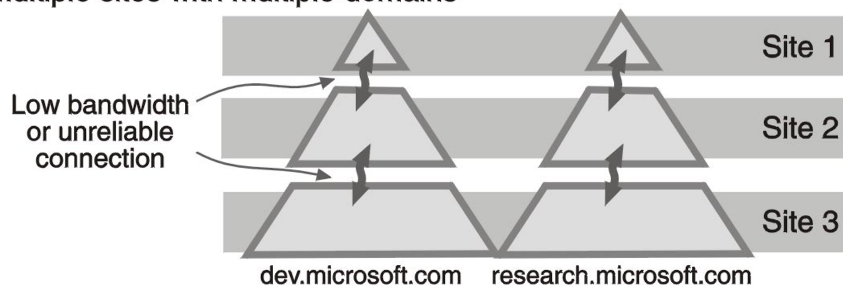
השתמש בהנחיות הבאות בעת מיזוג Subnets ליצירת Site :

- שלב רק תת-רשתות להן חיבורי רשת אמינים, זולים ומהירים. חיבורי רשת "מהירים" הם בעלי מהירות של לפחות 512Kbps, עבור רוחב פס בלתי מנוצל שניתן להקדיש לתעבורת שכפול. מומלץ לשקול בחיוב חיבורים בעלי רוחב פס גדול בהרבה עבור קישור לאתר בודד.
- הגדר אתרים כך שהשכפול יתרחש בזמנים שלא יפריעו לביצועי הרשת.

מבנה domain ומבנה אתר מתוחזקים בנפרד בשירותי Active Directory. domain בודד יכול לחצות אתרים רבים, ואתר בודד יכול להכיל domains או חלקים של domains (תרשים 6.4).







תרשים 6.4

A single domain with a single site, a single domain with multiple sites, and multiple sites with multiple domains.

מיטוב תעבורת התחברות של תחנות עבודה

בעת תכנון אתרים, שקול באיזה DCs ישתמשו תחנות העבודה של כל תת-רשת. כדי שתחנות עבודה תתחבר לקבוצה מסוימת של DCs, הגדר את ה-Sites כך שרק םDCs אלה יהיו באותו Site שבו נמצאת תחנת העבודה.

שכפול ספריית הרשת באופן אופטימלי

בעת תכנון אתרים, שקול את מיקום ה-DCs. כיון שכל DC משתתף בשכפול ה-Directory יחד עם ה-DCs האחרים ב-domain שלו, עליך להגדיר אתרים כך שהשכפול יתרחש במועדים או ברווחי זמן שלא יפריעו לביצועי הרשת.

הטבלה להלן מראה מתי יש ליצור אתר במיקום פיזי של החברה, בהתבסס על מספר תחנות העבודה באותו מקום.

תחנות עבודה	צור אתר?	הערות
אחת עד חמש	לא	משתמשים מאומתים על פני חיבור איטי. החיבור האיטי לא יחויב בתעבורת שכפול Domain.
יותר מחמש	כן	מקם DCs באופן מקומי, כדי להאיץ את תהליך אימות המשתמשים באתר המקומי. ניתן להגדיר תעבורת שכפול כך שתתרחש על פני חיבורים איטיים בזמני רגיעה, ובתדירות נמוכה יותר.

סיכום שיעור

בעת הכנה ליישום Active Directory Services, יש לתכנן בקפידה את מבנה Namespace (טווח השמות), ה-OUs (היחידות הארגוניות) וה-Sites (אתרים). תידרש לקבוע אם טווח השמות הפנימי וטווח השמות החיצוני זהים, או שונים. אם טווחי השמות זהים, אותו שם domain ברמת-על יופיע משני עברי קיר המגן (Firewall). אם טווחי השמות שונים, שם domain ברמת העל בצד הפנימי של קיר המגן שונה משם domain רמת העל מחוץ לקיר המגן. בנוסף לטווח השמות, עליך לתכנן גם את ה-OUs (יחידות ארגוניות). היחידות הארגוניות צריכות לשקף את פרטי המבנה העסקי של החברה, ולמפות את צורת העבודה וארגון העסק. עליך גם לתכנן את ה-sites (אתרים) שלך בקפידה לפני יישום Active Directory Services. בעת תכנון אתר, שלב רק Subnets להן חיבורי רשת זולים, אמינים ובעלי רוחב-פס גדול. יש להגדיר אתרים כך שהשכפול יתרחש במועדים שאינם מפריעים לביצועי הרשת.

שיעור 3: יישום
Active Directory Services

שיעור זה עוסק בנושא התקנת Active Directory Services במחשב Windows 2000 Server וכולל סקירה של אשף התקנת Active Directory. בנוסף, השיעור דן ב-shared system volume של מסד הנתונים, הנוצר בעת התקנת Active Directory Services. לבסוף השיעור דן בקובץ Ntds.dit ומצבי תחומים.

לאחר שיעור זה, תוכל

- **להתקין** Active Directory Services **על מחשב** Windows 2000 Server

זמן לימוד משוער: 30 דקות

אשף ההתקנה של Active Directory

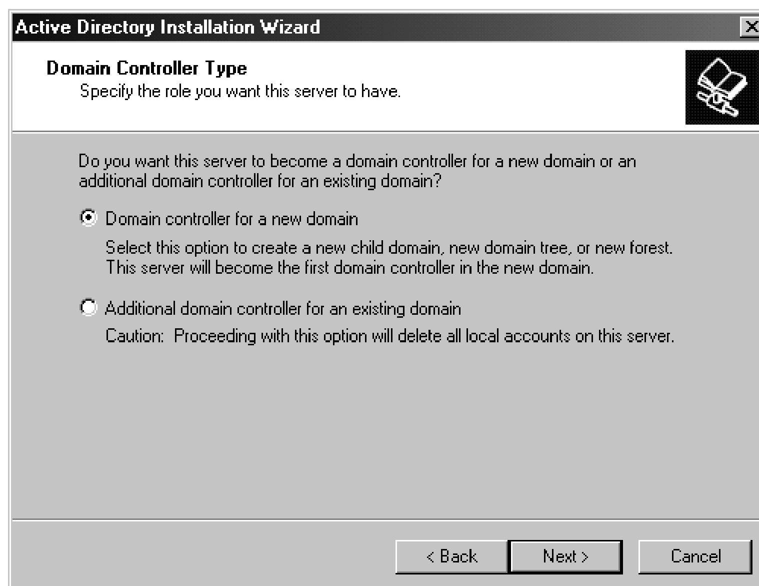
אשף ההתקנה של Active Directory משמש לביצוע המטלות הבאות:

- ❖ הוספת Domain Controller ל-Domain קיים.
- ❖ יצירת Domain Controller ראשון ב-Domain חדש.
- ❖ יצירת Child domain חדש.
- ❖ יצירת Domain tree חדש.

לטעינת אשף ההתקנה של Active Directory, הפעל את Configure Your Server, הנמצא בתפריט Administrative Tools שבתפריט Start, ובחר בקישור Active Directory. כעת תוכל להפעיל את אשף ההתקנה של Active Directory. תוכל גם להפעיל את אשף ההתקנה על ידי הפעלת תוכנית שירות dcpromo.exe מחלון Run או משורת הפקודה. כל אחת משיטות אלו תפעיל את אשף ההתקנה של Active Directory על שרת Standalone (עצמאי) ותנחה אותך בהתקנת Active Directory Services במחשב וביצירת DC חדש.

הערה במערכת Windows NT 4 לא היה ניתן להפוך שרת Standalone ל-Domain Controller מבלי להתקינו מחדש.

בעת התקנת Active Directory Services, תוכל לבחור להוסיף DC חדש ל-Domain קיים, או ליצור את DC ראשון ל-Domain חדש (תרשים 6.5).



תרשים 6.5 מסך Domain Controller Type באשף ההתקנה של Active Directory.

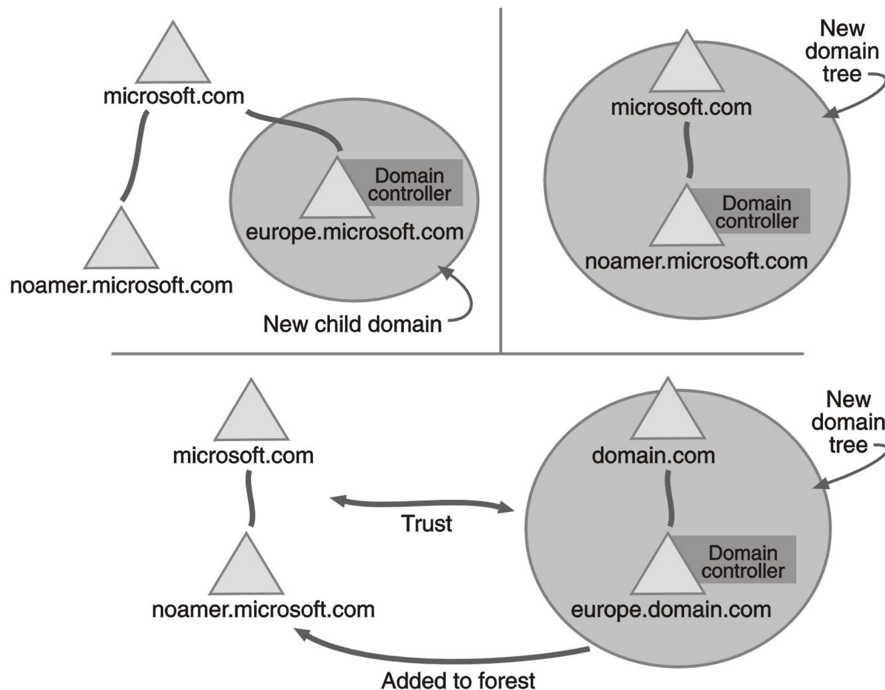
הוספת DC ל-Domain קיים

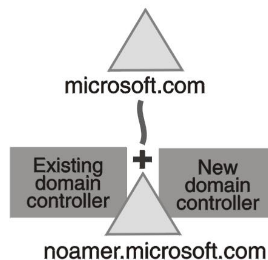
אם תבחר להוסיף Domain Controller ל-Domain קיים, צור Peer Domain Controller. יצירתם נועדה לשם יתירות (Redundancy) ולהפחתת העומסים על DCs קיימים.

יצירת DC ראשון ל-Domain חדש

אם תבחר ליצור DC ראשון ל-domain חדש, לא רק שתיצור DC חדש, אלא גם Domain חדש. יש ליצור Domains לחציצת מידע, דבר המאפשר לשנות את מימדי Active Directory Services כדי לענות לצרכי ארגונים גדולים במיוחד.

בעת יצירת Domain חדש, תוכל לבחור אם ליצור Child domain חדש או domain tree חדש. בעת יצירת Child domain, ה-Domain החדש מתוסף כ-child domain ל-Domain קיים. בעת יצירת Domain tree חדש, ה-Domain החדש אינו מהווה חלק מ-Domain קיים. בשלב זה, תוכל ליצור Forest (יער) חדש של Domain trees או להצטרף ליער קיים.





תרשים 6.6 מצגת גרפית של סוגים שונים של Domain Controllers.

אזהרה הפעלת dcpromo.exe על DC מאפשרת הסרת Active Directory Services מ-DC ובכך להורידו לרמת שרת עצמאי. אם תסיר את שירותי Active Directory מכל ה-DCs שב-Domain, **יימחק גם מסד הנתונים של ספריית הרשת מה-Domain, ועקב כך ה-Domain לא יתקיים יותר.**

The Database Shared System Volume

בעת התקנת שירותי Active Directory, נוצרים מסד הנתונים, יומן מסד הנתונים, קבצי יומן הנתונים ו-shared system volume, באופן אוטומטי.

מסד הנתונים של Active Directory

מסד הנתונים הוא ה-Directory של ה-Domain החדש. מיקום ברירת המחדל של מסד הנתונים וקבצי יומן מסד הנתונים הוא systemroot%\Ntds%. אולם, תוכל לציין מיקום אחר בעת התקנת Active Directory. לקבלת הביצועים הטובים ביותר, התקן את מסד הנתונים וקובץ היומן על דיסקים נפרדים. שקול להתקין את מסד הנתונים על אשכול דיסקים (**R**edundant **A**rray of **I**ndependent **D**isks - RAID) מסוג RAID-5 או RAID-10 לקבלת Fault tolerance ולשיפור ביצועים.

מסד הנתונים של ה-Directory (ספריית הרשת) מאוחסן בעצם בקובץ בשם Ntds.dit. קובץ Ntds.dit מכיל את כל המידע המאוחסן ב-Active Directory store. הוא מסד נתונים מסוג ESE (שיטת גישה באמצעות אינדקס רציף) ומכיל את הסכמה כולה, את הקטלוג הגלובלי ואת כל האובייקטים המאוחסנים על DC זה. בהליך הקידום, Ntds.dit מועתק מתיקיה systemroot%\System32% לתיקיה המיועדת. שירותי Active Directory מופעלים עתה מהעתק הקובץ החדש, ואם נוכחים DCs נוספים, הליך השכפול מעדכן קובץ זה מ-DCs אחרים.

Shared System Volume

Shared System Volume הוא מבנה תיקיה הקיים בכל ה-DCs של Windows 2000. הוא מאחסן קוד תוכנה וכמה מהאובייקטים של מדיניות הקבוצה (Group Policy) עבור ה-domain הנוכחי כמו גם עבור החברה כולה. מיקום ברירת המחדל של מחיצת המערכת המשותפת הוא systemroot%\Sysvol%. Shared System Volume חייבת להיות מותקנת על volume שפורמט עם NTFS 5.0.

שכפול Shared System Volume מתרחש באותו מועד בו משוכפל ה-Active Directory. כתוצאה מכך, ייתכן שלא תרגיש בשכפול הקבצים אל system volume חדשה שנוצרה זה עתה וממנו, עד שיחלפו שתי תקופות השכפול (בדרך כלל 10 דקות). זאת כי תקופת השכפול הראשונה מעדכנת את תצורת ה-system volumes האחרות כך שהם מודעים ל-system volume החדשה שנוצרה זה עתה.

Domain Modes

ישנם שני מצבי Domain: Mixed Mode (מצב מעורב) Native Mode (מצב טהור).

Mixed Mode

בעת התקנה או שדרוג ראשוני של DC ל-Windows 2000 Server, ה-DC פועל ב-Mixed Mode (מצב מעורב). מצב מעורב מאפשר ל-DC לתקשר עם כל ה-DCs שב-domain, הפועלים תחת מערכות הפעלה Windows NT 3.51/4.0 (DCs ברמה נמוכה יותר). בנוסף, כל לקוח המשתמש ב-NTLM ובשירות ספריית הרשת ב-Windows NT 3.51 ו-Windows NT 4.0 חייבים מצב מעורב לאימות הרשת. כמו כן הם צריכים WINS לשימוש בשמות. לקוחות ברמה-נמוכה אלה, בדרך כלל יעשו אימות מול מחשבי Windows 2000 Server לפני ש-Windows NT Server ברמה נמוכה יענה לבקשת ההתחברות שלהם. כמו כן, מחשב Windows 2000 Server תמיד ינצח בבחירה להיות Master Browser. התנהגות משולבת זו מוסיפה לחץ על DCs של Windows 2000 Server.

Native Mode

כאשר כל ה-DCs ב-Domain פועלים תחת Windows 2000 Server, ואינך מתכוון להוסיף DCs ברמה נמוכה יותר ל-Domain, ניתן להעביר את ה-domain מ-Mixed Mode (מצב מעורב) ל-Native Mode (מצב טהור).

בעת מעבר מ- Mixed Mode ל- Native Mode מתרחשים מספר דברים:

- התמיכה בשכפול ברמה-נמוכה מפסיקה. כיון ששכפול ברמה נמוכה נעלם, לא תוכל להחזיק DCs ב-domain שלך שאינם מפעילים Windows 2000 Server.
- לא ניתן להוסיף יותר DCs ברמה נמוכה ל-Domain.
- השרת ששימש כ-PDC בזמן ההמרה אינו Domain master יותר; כל ה-DCs מתחילים להתנהג באופן שיוויני.

הערה השינוי מ- Mixed Mode ל- Native Mode הוא **חד-כיווני בלבד**; **לא ניתן לשנות** מ- Native Mode **ל-** Mixed Mode.

הערה ב-Windows 2000 Server **אין צורך יותר בחלוקה ל-**PDC **ול-**BDC. כל ה-DCs **שוים** מבחינת הרשת.

תרגיל 1 : התקנת Active Directory Services

בתרגיל זה, תהפוך את השרת העצמאי Server01, ל-DC הראשון בעץ Active Directory. ההתקנה תתקין ותגדיר DNS לתמיכה ביישום שמות. בפרק מאוחר יותר תלמד עוד על DNS ושירותי רשת אחרים, כגון Dynamic Host Configuration Protocol (DHCP), פרוטוקול דינמי להגדרת מארח). השלם את כל ההליכים בתרגיל זה על Server01.

הליך 1 : קידום שרת Standalone ל- Domain Controller

בתרגיל זה, תפעיל dcpromo.exe להתקנת Active Directory Services ו-DNS על השרת העצמאי (Server01), ובכך תהפכו ל- DC ושרת DNS ב-Domain חדש.

1. הפעל את Server01 והיכנס בשם משתמש Administrator עם הסיסמה password.
2. אם ייפתח דף Windows 2000 Configure Server, סגור אותו, כיון שתוכנית dcpromo.exe תשמש במקומו לביצוע המשימות בהליך זה.
3. הכנס את תקליטור ההתקנה של Windows 2000 Server לכונן התקליטורים ב-Server01.

   תקליטור ההתקנה נדרש להתקנת שירות DNS בעת פעולת dcpromo.exe.
4. אם יופיע אשף Windows 2000, לחץ Exit לסגירת המסך.
5. לחץ Start ואחר כך Run.
6. בתיבת הדו-שיח של Run, הקלד **dcpromo.exe** ולחץ OK. יופיע אשף ההתקנה של Active Directory.
7. לחץ Next. יופיע מסך Domain Controller Type.
8. בחר Domain Controller For A New Domain, ולחץ Next. יופיע מסך Create Tree OR Child Domain.
9. ודא בחירת לחצן אפשרויות Create A New Domain Tree, ולחץ Next. יופיע מסך Create Or Join A Forest.
10. בחר בלחצן אפשרויות Create A New Forest Of Domain Trees, ולחץ Next. יופיע מסך New Domain Name.
11. בתיבה Full DNS Name For The New Domain, הקלד **microsoft.com**, ולחץ Next. לאחר מספר דקות יופיע מסך NetBIOS Domain Name.
12. ודא ש-MICROSOFT מופיע בתיבת הטקסט Domain NetBIOS Name, ולחץ Next. יופיע מסך Database And Log Locations.

13. ודא שגם מסד הנתונים וגם היומן ממוקמים ב-C:\Winnt\Ntds, ולחץ Next. יופיע מסך Shared System Volume.

14. קרא את המידע המופיע על מסך Shared System Volume, ודא ש-SYSVOL ממוקם ב-C:\WINNT\SYSVOL.

15. לחץ Next. תופיע תיבת הודעות של אשף ההתקנה של Active Directory, המודיעה שלא ניתן לאתר DNS עבור microsoft.com.

16. לחץ OK. Dcpromo לא מצא DNS זמין עבור microsoft.com, וכתוצאה מכך יופיע מסך Configure DNS.

17. ודא שלחצן Yes, Install And Configure DNS On The Computer (Recommended) נבחר, ולחץ Next. מסך Permissions יופיע.

18. תחילה, ה-DC יופעל במצב מעורב, כך שיש לוודא שלחצן אפשרויות Permissions Compatible With Pre-Windows 2000 Servers נבחר, ולחץ Next.

    יופיע מסך Directory Services Restore Mode Administrator Password.

19. קרא מסך זה והקלד **password** בשתי תיבות הטקסט, ולחץ Next. יופיע מסך Summary, ובו רשימת האפשרויות שבחרת.

20. בחן את תוכן מסך התמצית ולחץ Next.

    מחוון ההתקדמות Configuring Active Directory יופיע בעוד שירותי Active Directory מותקנים על השרת.

    הליך זה יארך מספר דקות. בעודך ממתין, ודא שהכנסת את תקליטור ההתקנה של Windows 2000 Server ל-Server01, כהכנה להתקנת שירות DNS.

21. כאשר יופיע מסך אשף Completing The Active Directory Installation, הוצא את התקליטור, לחץ Finish, ואז לחץ Restart Now.

    בפעם הראשונה שמערכת Windows 2000 Server תופעל כ-DC, משך האתחול שלה יהיה ארוך מהרגיל.

הליך 2: צפייה ב-Domain שלך

בהליך זה, תצפה ב-Domain שלך.

1. היכנס ל-Server01 בשם משתמש Administrator עם הסיסמה password.
2. לחץ לחיצה כפולה על My Network Places. יופיע חלון My Network Places.
3. לחץ לחיצה כפולה על Entire Network, ולחץ על הקישור שבצד שמאל של החלון עם הכיתוב You May Also View The Entire Contents Of The Network.
4. לחץ לחיצה כפולה על Microsoft Windows Network. שים לב שרשת Microsoft מופיעה.
5. סגור את My Network Places.

הליך 3: שימוש ב- Active Directory Manager

בהליך זה, תשתמש בתוסף התוכנה Active Directory Users And Computers לצפייה ב-domain שלך.

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ואז לחץ על Active Directory Users And Computers.

   יופיע תוסף התוכנה Active Directory Users And Computers.
2. בחלון Tree, לחץ על סימן + שמשמאל ל-microsoft.com.
3. בחן כל מכולה שמתחת ל-microsoft.com. אין לשנות אף נתון בצמתים אלה.

   איזה בחירות מופיעות ברשימה תחת microsoft.com ומה מטרתן? רמז: בחר בתכונות של כל מכולה בחלון Tree כדי לעיין במטרתן.

תרגיל 2: חיבור Server02 ל-Domain

בתרגיל זה, יצטרף Server02 ל-Domain microsoft.com. כיון ש- DHCP לא בשימוש בשלב זה של ההדרכה, תיאלץ להגדיר כתובת IP בצורה ידנית על Server01 ו-Server02. כאשר Server02 מצטרף ל-Domain, ייווצר חשבון מחשב עבור Server02. חשבון מחשב זה יופיע ב-Active Directory store. שני המחשבים ישמשו להשלמת תרגיל זה.

הליך 1: הגדרה ידנית של מיעון IP וצירוף Server02 ל-Domain microsoft.com.

1. בשרתים Sever01 ו-Server02, היכנס בשם משתמש Administrator עם הסיסמה password.
2. בשרת Server01, לחץ Start, הצבע על Settings, ולחץ על Network And Dial-Up Connections. יופיע חלון Network And Dial-Up Connections.
3. לחץ Local Area Connection ומתפריט File, לחץ Properties. תופיע תיבת הדו-שיח Local Area Connection Properties.
4. בתיבת סימון Components Checked Are Used By This Connection, לחץ על Internet Protocol (TCP/IP).
5. לחץ Properties. תופיע תיבת דו-שיח Internet Protocol (TCP/IP) Properties.
6. לחץ על לחצן אפשרויות Use The Following IP Address (השתמש בכתובת IP הבאה).
7. בתיבת כתובת IP הקלד: **10.10.10.1.**
8. בתיבה Subnet Mask, ודא שמופיע 255.0.0.0.
9. לחץ על לחצן אפשרויות Use The Following DNS Server Addresses.
10. בתיבה Preferred DNS Server (שרת DNS מועדף) הקלד **10.10.10.1.**
11. לחץ OK.
12. תופיע תיבת דו-שיח Local Area Connection Properties.
13. לחץ OK.
14. בשרת Server02, לחץ Start, הצבע על Settings, ולחץ Network And Dial-Up Connections.
15. יופיע חלון Network And Dial-Up Connections.
16. לחץ Local Area Connection, ומתפריט File, לחץ Properties. תופיע תיבת דו-שיח Local Area Connection Properties.

17. בתיבה Components Checked Are Used By This Connection, לחץ Internet Protocol (TCP/IP).

18. לחץ Properties. תופיע תיבת דו-שיח Internet Protocol (TCP/IP) Properties.

19. לחץ על לחצן אפשרויות Use The Following IP Address.

20. בתיבת כתובת IP הקלד : **10.10.10.2.**

21. בתיבה Subnet Mask, ודא שמופיע 255.0.0.0.

22. לחץ על לחצן אפשרויות Use The Following DNS Server Addresses.

23. בתיבה Preferred DNS Server הקלד **10.10.10.1**.

24. לחץ OK. תופיע תיבת דו-שיח Local Area Connection Properties.

25. לחץ OK.

26. פתח את Console בשרת Server02.

27. בחר בכרטיסיה Network Identification, ולחץ Properties. תופיע תיבת הדו-שיח Identification Changes.

28. לחץ על לחצן האפשרויות Domain, הקלד **microsoft,** ולחץ OK. תופיע תיבת הדו-שיח Domain Username And Password.

29. בתיבת הטקסט Name, הקלד **Administrator**, ובתיבת הטקסט Password, הקלד **password**. לחץ OK. לאחר מספר דקות, תופיע תיבת הודעות Network Identification, המברכת אותך לרגל כניסתך ל-Domain.

30. לחץ OK. תיבת ההודעה Network Identification תנחה לכבות את המחשב ולחזור ולהפעיל אותו, כדי שהשינויים יקבלו תוקף.

31. לחץ OK. תופיע תיבת דו-שיח System Properties.

32. לחץ OK. תיבת ההודעות System Settings Change תנחה שיש לכבות ולחזור ולהפעיל את המחשב כדי שהשינויים יקבלו תוקף.

33. לחץ Yes לכבות את המחשב, לחזור ולהפעיל אותו.

34. בשרת Server02, היכנס ל-microsoft.com domain בשם משתמש Administrator עם הסיסמה password.

35. אם יופיע מסך Configure Your Server, הסר סימון מתיבת הסימון Show This Screen At Startup וסגור את המסך.

תרגיל 3: התקנת Adminpak.msi ובחינת התכולה שלה

בתרגיל זה, תכין תחילה רשימה של הכלים המופיעים תחת הקבוצה Administrative Tools, ואז תתקין את Adminpak.msi לקביעת הכלים הנוספים שיותקנו על ידי שגרת ההתקנה של כלי הניהול. בצע את כל ההליכים בתרגיל זה על Server01.

הליך 1: כיוון הגדרות תפריט ההתחלה (Start), ובחינת כלים חדשים שהותקנו תחת Administrative Tools (כלי ניהול)

בהליך זה תבטל את התכונה המציגה רק את הפריטים השמישים ביותר (Most Used) שבתפריט התחלה Start.

1. בשרת Sever01, היכנס בשם משתמש Administrator עם הסיסמה password.
2. לחץ Start, הצבע על Settings, ופתח את Taskbar And Start Menu. תופיע תיבת הדו-שיח Taskbar and Start Menu Properties.
3. לחץ על תיבת סימון Use Personalized Menus, ולחץ OK.
4. לחץ על לחצן Start, הצבע על Programs, והצבע על Administrative Tools.

שים לב שכל היישומים של כלי הניהול המותקנים מופיעים תחת Administrative Tools, ולא רק יישומים בהם השתמשת לאחרונה.

כאשר שרת Server01 היה שרת עצמאי, כל היישומים הופיעו תחת Administrative Tools פרט לאלה הייחודיים ל-Windows 2000 Server, תחומים, ותחזוקת DNS. השתמש בעכבר והצבע על כל אחד מהיישומים המופיעים מטה כדי לראות את תיאור המסך.

Active Directory Domain and Trusts

Active Directory Sites and Services

Active Directory Users and Computers

DNS

הליך 2: התקנת כלי ניהול נוספים

בתרגיל זה, תתקין את Windows 2000 Administrative Pack על שרת Server01. כלים אלה ניתן גם להתקין על Windows 2000 Professional לסייע בניהול מרחוק של Windows 2000 Server.

1. פתח את תפריט Start, ולחץ Run. תיבת הדו-שיח Run תופיע.
2. הקלד **adminpak.msi**.

Adminpak.msi מותקן ב: C:\WINNT\system32, שהוא נתיב החיפוש. לכן אין צורך להקליד את הנתיב עבור קובץ התקנה זה של Microsoft.

3. לחץ OK. לאחר זמן מה, יופיע אשף Windows 2000 Administration Tools.
4. קרא את המידע המופיע על המסך, ולחץ Next. יופיע מסך Setup Options.
5. לחץ על לחצן אפשרויות Install All Of The Administrative Tools, ולחץ Next. יופיע מסך התקדמות ההתקנה, בעוד כלי הניהול מותקנים.
6. כאשר יופיע מסך אשף Completing The Windows 2000 Administration Tools Setup, לחץ Finish להשלמת ההתקנה.
7. עיין בכלים הנוספים המופיעים תחת Administrative Tools. לראות מה היעוד של כל כלי, הצב את סמן העכבר מעל הכלי החדש, כדי להציג תיאור כלי.

תרגיל 4: שינוי מ- Standalone Dfs ל- Domain Dfs

בפרק 3, התקנת Microsoft **D**istributed **F**ile **S**ystem - Dfs. בפרק זה, תמחק את ה-Standalone Dfs, תיצור Domain Dfs ותיצור שכפול של שורש Dfs, כיון שכעת אתה מפעיל Domain Controller. השרתים Server01 ו-Server02 ישמשו להשלמת ההליכים בפרק זה.

הליך 1: מחיקת שורש Standalone Dfs

רק שורש Dfs אחד יכול להתקיים על שרת. אי לכך, ה- Standalone Dfs של Server01 חייב להימחק.

1. לחץ על לחצן Start, הצבע על Programs, והצבע על Administrative Tools.
2. בקבוצה Administrative Tools, לחץ על Distributed File System. תוסף התוכנה Distributed File System יופיע.
3. בחלון Tree, לחץ \\SERVER01\Public.

4. פתח את תפריט Action, ולחץ על Delete Dfs Root. תופיע תיבת הודעות של Distributed File System המודיעה שמחיקת שורש Dfs, מבטלת אפשרות גישה חוזרת ל-Dfs. הליך זה אינו מוחק את השיתופים שהיו מקושרים לשורש Dfs.
5. לחץ Yes.

הליך 2: יצירת Domain Dfs

Domain Dfs יוגדר בדומה ל- Standalone Dfs, אך הוא ייצור שכפול קבצים לשכפולי הקישורים של Dfs. בצע הליך זה על Server01.

1. בחלון Tree של תוסף התוכנה Distributed File System, לחץ Distributed File System.
2. פתח את תפריט Action, ולחץ New Dfs Root. אשף New Dfs Root יופיע.
3. לחץ Next. מסך Select the Dfs Root Type יופיע.
4. בחר לחצן אפשרויות Create A Dfs Root, ולחץ Next.

מסך Select The Host Domain For The Dfs Root יופיע, והשם microsoft.com יופיע בתיבת הטקסט Domain Name ובתיבה Trusting Domains.

5. לחץ Next. מסך Specify The Host Server For The Dfs Root יופיע.
6. שים לב שהשם Server01.microsoft.com מוצג בתיבת הטקסט Server Name.

אם Server01 היה מארח עדיין את ה-Dfs העצמאי, שמו לא היה נכתב בתיבת הטקסט Server Name. דבר זה נעשה בכוונה, כיון ששרת יכול לארח רק שורש Dfs אחד.

7. לחץ Next. יופיע מסך Specify The Dfs Root Share.
8. ודא שלחצן אפשרויות Use An Existing Share מסומן, ומתיבת הרשימה הנפתחת, בחר Public.
9. לחץ Next.
10. בתיבת הטקסט Comment המופיעה במסך Name The Dfs Root, הקלד **Public Access Share**, ולחץ Next.
11. עיין בהגדרות המופיעות על מסך אשף Completing The New Dfs Root. שים לב שהשרת המארח הוא SERVER01.microsoft.com. כאשר יצרת שורש Dfs עצמאי, שם השרת המארח היה SERVER01.
12. לחץ Finish. תוסף התוכנה Distributed File System Manager יופיע, ושורש Dfs יוגדר על SERVER01.microsoft.com, ויופיע כ-\\microsoft.com\Public.

הליך 3: יצירת העתק שורש Dfs

בהליך הבא, תיצור העתק שורש Dfs של SERVER01\Public\\ על שרת Server02. Server02 צורף לdomain- microsoft.com בתרגיל 2.

1. מחלון Tree של תוסף התוכנה Distributed File System בשרת Server01, בחר microsoft.com\Public\\. שורש Dfs בשם SERVER01\Public\\ יופיע בחלונית הימנית.
2. פתח את תפריט Action, ולחץ New Root Replica.

   יופיע מסך Specify The Host Server For Dfs Root.
3. בתיבת הטקסט Server Name, הקלד **Server02** ולחץ Next. ניתן לשכפל שורש Dfs של domain לשרת אחר (DC או member server) ב-domain.

   יופיע מסך Specify The Dfs Root Share.
4. בחר לחצן אפשרות Create A New Share.
5. בתיבת הטקסט הקש בחר c:\publicrepl.
6. בתיבת שם השיתוף (Share Name) הקש pubrepl.
7. לחץ Finish. תופיע תיבת ההודעות של מערכת הקבצים המבוזרת והיא תציין ש-Server02\c$\publicrepl\\, אינו קיים.
8. לחץ Yes ליצירת התיקיה.

הליך 4: הפעלת FRS להעתק שורש Dfs

בהליך זה תאפשר מדיניות שכפול, כך ששורש Dfs יותאם אוטומטית עם ההעתק שלו.

1. בשרת Server01, בחר \\microsoft.com\Public מחלון Tree של תוסף התוכנה Distributed File System. בחלונית הימנית יופיע שורש Dfs בשם \\SERVER01\Public וגם \\SERVER02\pubrepl.
2. פתח את תפריט Action, ולחץ על Replication Policy. תופיע תיבת הדו-שיח של Replication Policy.
3. לחץ על \\SERVER01\Public, ולחץ Set Master.
4. לחץ \\SERVER02\Pubrepl, ולחץ Enable כדי לאפשר שכפול.
5. לחץ OK לסגירת תיבת הדו-שיח Replication Policy.

הליך 5: יצירת קישורי Dfs

בהליך זה תיצור מחדש את קישורי Dfs שיצרת בפרק 3, תרגיל 1, הליך 3.

1. בשרת Server01, בחר \\microsoft.com\Public מחלון Tree של תוסף התוכנה Distributed File System. בחלונית הימנית יופיע שורש Dfs בשם \\SERVER01\Public וגם \\SERVER02\pubrepl.
2. פתח את תפריט Action, ולחץ New Dfs Link.

   תופיע תיבת דו-שיח Create A New Dfs Link.
3. בתיבת הטקסט Link Name, הקלד **Intranet.**
4. בתיבת הטקסט Send The User To This Shared Folder (שלח את המשתמש לתיקיה משותפת זו), הקלד **\\Server02\internal.**
5. בתיבת הדו-שיח Comment, הקלד **Internal web content**, ולחץ OK.
6. חזור על שלבים 3-8 ליצירת קישורי Dfs חדשים תוך התייחסות למידע המופיע בטבלה להלן:

שם קישור	שלח את המשתמש לתיקיה משותפת זו	הערה
news	\\Server01\Press	הודעות עדכניות לעיתונות
ftp	\\Server01\ftproot	ספריית שורש FTP
tech	\\Server01\TechDocs	אזור מסמכים טכניים

7. בשרת Server02, פתח את C:\Publicrepl (העתק שורש Dfs), ותראה שהעתקים חדשים של התיקיות מופיעים תחת שורש Dfs.

סיכום שיעור

אשף ההתקנה של Active Directory משמש להתקנת שירותי Active Directory על מחשב Windows 2000 Server. אשף ההתקנה של Active Directory משמש גם להוספת DC ל-domain קיים, ליצירת DC ראשון ב-domain חדש, יצירת Child domain חדש, או יצירת domain tree חדש. בעת התקנת שירותי Active Directory, מסד הנתונים, קבצי היומן של מסד הנתונים, ו-shared system volume, נוצרים באופן אוטומטי. מסד הנתונים של ספריית הרשת שמור בקובץ בשם Ntds.dit. קובץ Ntds.dit מכיל את Active Directory store. Shared System Volume הוא מבנה תיקיות הקיים בכל ה-DCs של Windows 2000. הוא מאחסן קודים כתובים וכמה מהאובייקטים של מדיניות הקבוצה של ה-Domain הנוכחי וגם של הארגון. ישנם שני מצבי Domain : Mixed Mode (מצב מעורב) ו- Native Mode (מצב טהור). בעת התקנה או שדרוג DC ל-Windows 2000 Server לראשונה, ה-DC פועל ב- Mixed Mode. לאחר שכל ה-DCs ב-domain מפעילים את Windows 2000 Server, ואינך מתכוון להוסיף עוד DCs ברמה נמוכה (שאינם Windows 2000 Server) ל-Domain, תוכל להעביר את ה-Domain מ- Mixed Mode ל- Native Mode.

שיעור 4: ניהול
Active Directory Services

לאחר שהתקנת את שירותי Active Directory, אתה ערוך ליצירה וניהול האובייקטים המאוחסנים בשירות ספריית הרשת. שיעור זה מסביר את הליך יצירת יחידות ארגוניות (OU) והוספת אובייקטים ליחידות אלה. לאחר מכן, מוסיף השיעור ומפרט כיצד לנהל אובייקטים אלה כך שתוכל לאתר, לשנות ולמחוק אובייקטים כנדרש. לבסוף השיעור דן בנושא בקרת גישה לאובייקטים אלה, הכולל ניהול הרשאות Active Directory והאצלת סמכויות ניהול אובייקטים.

לאחר שיעור זה, תוכל

- ליצור יחידות ארגוניות ואת האובייקטים שלהם.
- לאתר, לשנות, להעביר ולמחוק אובייקטים שיצרת.
- לבקר גישה לאובייקטים של Active Directory.

זמן לימוד משוער: 35 דקות

יצירת OUs (יחידות ארגוניות) והאובייקטים שלהן

אובייקטים של Active Directory מייצגים משאבי רשת. כל אובייקט הוא ערכת מאפיינים ייחודית בעלת שם, המייצגת משאב רשת מסוים. בעת הוספת משאבים חדשים לרשת, כגון חשבונות משתמשים, קבוצות, או מדפסות, אתה יוצר אובייקטים חדשים של Active Directory המייצגים משאבים אלה.

לפני הוספת אובייקטים לשירותי Active Directory, יש ליצור את ה-OUs שיכילו אובייקטים אלה.

יצירת OUs

ניתן ליצור OU (יחידה ארגונית) תחת Domain, תחת אובייקט DC, או בתוך יחידה ארגונית אחרת. לאחר שיצרת יחידה ארגונית, תוכל להוסיף לה אובייקטים.

ליצירת יחידות ארגוניות (**O**rganizational **U**nits - OUs), עליך להצטייד בהרשאות המתאימות להוספת יחידות ארגוניות בתוך היחידה הארגונית ההורה, ה-Domain, או Domain controller node בו נדרש ליצור את היחידה הארגונית. ברירת המחדל היא שלחברים בקבוצת Administrators יהיו הרשאות ליצירת יחידות ארגוניות. לא ניתן ליצור יחידות ארגוניות ברוב המכולות המובנות במערכת, כגון Computers ו-Users.

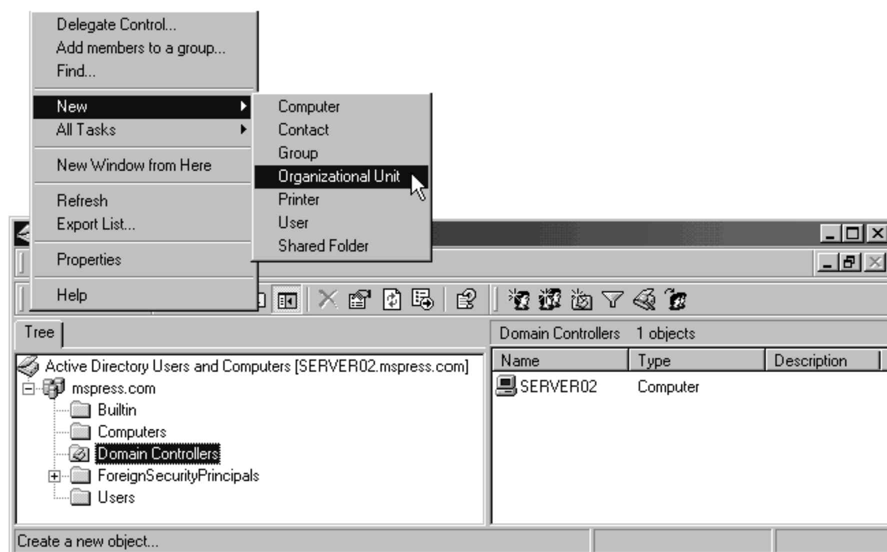
הערה המכולה המובנית היחידה מתחת למכולת ה-Domain **שניתן ליצור בתוכה** OUs **היא מכולת** Domain controller. **יש ליצור מכולות** OUs **ראשיות מתחת ל-**Domain **הרצוי, בהן ניתן ליצור** Child-OUs.

יחידות ארגוניות נוצרות לסייע בניהול הרשת (Network administration). מבנה היחידות הארגוניות צריך להיות מבוסס על צרכי הניהול הייחודיים שלך. אם נדרש, תוכל לשנות את מבנה היחידות הארגוניות בקלות, או להעביר אובייקטים בין יחידות ארגוניות.

עליך ליצור יחידות ארגוניות מהסיבות הבאות:

- להאצלת סמכויות ניהול למשתמשים או administrators אחרים.
- לקבץ אובייקטים הדורשים מטלות ניהול דומות. קיבוץ אובייקטים מאפשר למנהלים לאתר משאבי רשת דומים בקלות ולבצע את המטלות הניהוליות שלהם. לדוגמה, הם יכולים לקבץ את כל האובייקטים של משתמשים עבור עובדים זמניים באותה יחידה ארגונית.
- להגביל את החשיפה של משאבי הרשת ב-Active Directory. משתמשים יכולים לראות רק אובייקטים שנתת להם גישה אליהם. ניתן לשנות הרשאות של יחידות ארגוניות בקלות ולהגביל גישה למידע רשת סודי.

תוכל ליצור יחידה ארגונית בתוסף התוכנה Active Directory Users and Computers על ידי בחירת ה-domain או היחידה הארגונית הקיימת אשר בה תרצה ליצור את ה-OU (היחידה הארגונית) החדשה. משם, פתח את תפריט Action, הצבע על New, ולחץ על Organizational Unit (תרשים 6.7). הקלד את שם היחידה הארגונית בתיבת הטקסט Name, ולחץ OK.



תרשים 6.7 יצירת יחידה ארגונית בתוסף התוכנה Active Directory Users and Computers.

הוספת אובייקטים ל- OUs

להוספת אובייקטים ל- OUs (יחידות ארגוניות), חובה שיהיו לך ההרשאות הנדרשות ליצירת אובייקטים ביחידה הארגונית בה אתה רוצה את האובייקט. ברירת המחדל היא שלחברים בקבוצת administrators יש הרשאות ליצירת יחידות ארגוניות. האובייקטים הניתנים ליצירה מוכתבים על ידי הסכמה (Schema), האשף או תוסף התוכנה בו תשתמש. לעיתים, בעת יצירת אובייקט, לא כל המאפיינים זמינים להגדרה. ייתכנו מקרים בהם, כדי להגדיר את כל המאפיינים של אובייקט, עליך לשנות ולהתאים את האובייקט לאחר יצירתו.

הערה מאפייני אובייקטים בסכמה הם קטגוריות מידע, המגדירות את המאפיינים לכל סוג אובייקט מוגדר. כל סוג מסוים של אובייקט מוגדר הוא בעל אותם מאפיינים. ערכי המאפיינים של כל סוג אובייקט גורמים לכך שהוא יהיה ייחודי. לדוגמה, כל האובייקטים של משתמשים יהיו בעלי מאפיין **שם פרטי**; אולם, הערך של המאפיין **שם פרטי** יכול להיות כל שם, כמו לינדה או מקס.

תוכל ליצור אובייקטים בתוסף התוכנה Active Directory Users and Computers. בחר את היחידה ארגונית שאליה אתה רוצה להוסיף את האובייקט, פתח את תפריט Action, הצבע על New, ולחץ על שם סוג האובייקט שאותו אתה רוצה להוסיף. הכנס את המידע המתאים בתיבה/תיבות הדו-שיח שיופיעו.

תיאור אובייקטים של Active Directory

הוספת משאבים חדשים לרשת יוצרת אובייקטים חדשים של Active Directory המייצגים משאבים אלה. הטבלה הבאה מתארת את האובייקטים הנפוצים ביותר הניתנים להוספה לשירותי Active Directory:

סמל	אובייקט	תיאור
	Computer	אובייקט Computer מייצג מחשב ברשת. עבור תחנת עבודה Windows NT מחשבי Windows NT Server, זהו חשבון המחשב. האובייקט מכיל מידע אודות מחשב שהוא חבר ב-Domain.
	Contact	אובייקט Contact הוא חשבון שאין לו כל הרשאות אבטחה. לא ניתן להתחבר לרשת בתור Contact. ככלל, אנשי-קשר משמשים לייצוג משתמשים חיצוניים לצרכי דואר אלקטרוני.
	Group	אובייקט Group יכול להכיל משתמשים, מחשבים וקבוצות אחרות. קבוצות מפשטות את הניהול של מספר רב של אובייקטים.

סמל	אובייקט	תיאור
	Printer	אובייקט Printer הוא מדפסת רשת שפורסמה בספריית הרשת. האובייקט למעשה מהווה מצביע עבור מדפסת המחשב. יש לפרסם ידנית מדפסת במחשב שאינה תחת Active Directory Services.
	User	אובייקט User הוא עצם אבטחה בספריית הרשת. המידע באובייקט זה מאפשר למשתמש להתחבר ל-Windows 2000. המידע כולל גם שדות ברירה רבים, כמו שם פרטי, שם משפחה, שם תצוגה וכתובת דואר אלקטרוני.
	Shared Folder	אובייקט Shared Folder הוא שיתוף רשת שפורסם בספריית הרשת. האובייקט הוא למעשה מצביע לתיקיה משותפת. הוא כולל את כתובת הנתונים ולא את הנתונים עצמם. תיקיות משותפות מתקיימות ברישום המערכת. כאשר אתה מפרסם תיקיה בשירותי Active Directory, אתה יוצר אובייקט המכיל מצביע לתיקיה המשותפת.

תרגיל 5: יצירת OU והאובייקטים שלה

בתרגיל זה, תיצור חלק ממבנה ארגוני של Domain על ידי יצירת יחידה ארגונית. לאחר מכן תיצור שלושה חשבונות משתמשים שישמשו אותך בתרגיל מאוחר יותר.

הליך 1: יצירת OUs ואובייקטים של משתמשים

בהליך זה תיצור שתי יחידות ארגוניות ושלושה אובייקטים של משתמשים.

1. היכנס לשרת Server01 בשם משתמש Administrator עם הסיסמה password.
2. פתח את Active Directory Users And Computers. כדי לוודא שאתה יוצר יחידה ארגונית חדשה במיקום הנכון, עליך לבחור קודם את המיקום.
3. בחלון Tree, לחץ microsoft.com.
4. פתח את תפריט Action, הצבע על New ולחץ Organizational Unit. תופיע תיבת דו-שיח New Object - Organizational Unit.

   שים לב שהנתון היחיד הנדרש הוא השם. תיבת הדו-שיח מצביעה על המקום בו ייווצר האובייקט. מקום זה אמור להיות /microsoft.com.
5. בתיבה Name הקלד **Sales** ולחץ OK. היחידה הארגונית של Sales תופיע בחלון Tree.

6. תחת microsoft.com, צור יחידה ארגונית נוספת, בשם Servers.

7. בחלון Tree לחץ Users.

8. פתח את תפריט Action, הצבע על New, ולחץ על User.

שים לב שתיבת הדו-שיח New Object - User מראה שחשבון משתמש חדש נוצר בתיקיה User של microsoft.com/Users.

הערה ניתן ליצור חשבונות משתמשים בכל יחידה ארגונית. בהליך זה, תיצור את רוב האובייקטים של משתמשים ביחידה הארגונית Users. אולם, זו אינה דרישת חובה ליצירת אובייקטים.

---

9. צור חשבון משתמש חדש עם הנתונים הבאים :

שם בתיבת הטקסט	סוג
שם פרטי	Jane
שם משפחה	Doe
שם כניסה למערכת	Jane_Doe

10. לחץ Next.

11. השאר את שדות הסיסמה ריקים, אל תשנה את הגדרות ברירת המחדל לחשבון משתמש זה, ולחץ Next. מסך התמצית יופיע ובו יוצג השם המלא ושם ההתחברות Jane Doe.

12. לחץ Finish.

13. לחץ על הרשומה Jane_Doe בחלונית הימנית של תוסף התוכנה Active Directory Users And Computers.

14. פתח את תפריט Action ולחץ Properties. תיבת הדו-שיח Jane Doe Properties תופיע.

15. על הכרטיסיה General של תיבת הדו-שיח Jane Doe Properties, בתיבת הטקסט של הטלפון, הקלד 555-1234.

16. לחץ OK.

17. צור את חשבונות המשתמשים הבאים תחת האובייקט Users.

שם בתיבת הטקסט	סוג
שם פרטי	John
שם משפחה	Smith
שם כניסה למערכת	John_Smith

שם בתיבת הטקסט	סוג
שם פרטי	Bob
שם משפחה	Train
שם כניסה למערכת	Bob_Train

חשבונות משתמשים אלה ישמשו אותך בפרק הבא.

ניהול אובייקטים של Active Directory

הליך ניהול אובייקטים של Active Directory כרוך במספר מטלות שונות, כגון איתור אובייקטים, שינוי ומחיקת אובייקטים והעברת אובייקטים. לשינוי, מחיקה והעברת אובייקטים, עליך להיות בעל ההרשאות הנדרשות עבור האובייקט והיחידה הארגונית אליה אתה מעביר את האובייקט. כברירת המחדל, לחברים בקבוצת administrators יש את ההרשאות הנדרשות.

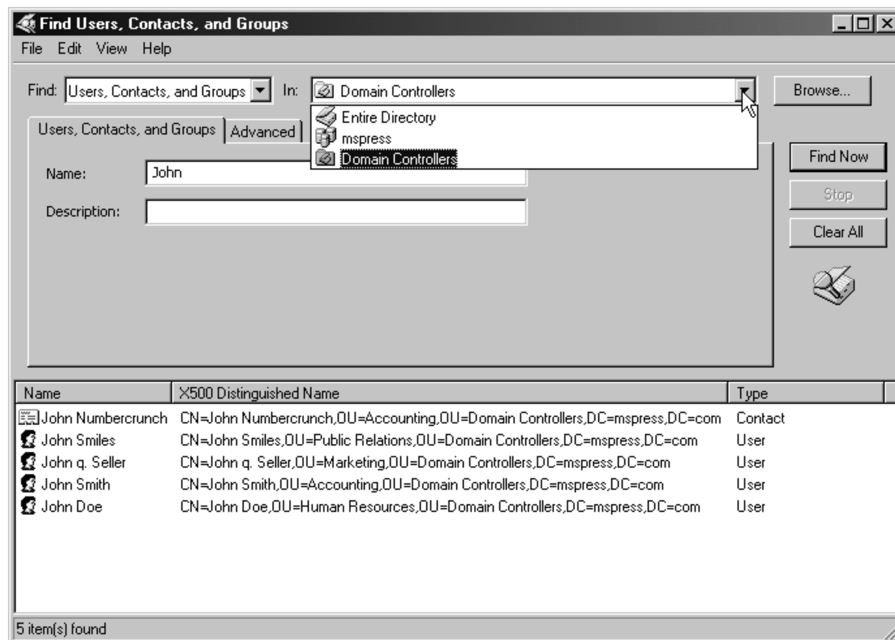
איתור אובייקטים

הקטלוג הגלובלי (Global Catalog) מכיל העתק חלקי של כל ה-Directory (ספריית הרשת), כך שהוא אוגר נתונים על כל אובייקט בעץ או ביער. כתוצאה מכך, משתמש יכול לאתר נתונים ללא תלות באיזה Domain בעץ או ביער שומר את המידע. תכולת הקטלוג הגלובלי מופקת אוטומטית על ידי שירותי Active Directory מהתחומים המרכיבים את ספריית הרשת.

לאיתור אובייקטים של Active Directory, פתח את תוסף התוכנה Active Directory Users And Computers הנמצא בתיקיית Administrative Tools. עתה לחץ לחיצה ימנית על domain או יחידה ארגונית בחלון Tree, ולחץ Find. תיבת הדו-שיח Find תופיע.

הערה אם תיגש לתפריט הקיצור של אובייקט תיקיה משותפת ותלחץ Find, פעולת האיתור של סייר Windows מופעלת, ותוכל לחפש בקבצים ובתיקיות.

תיבת הדו-שיח Find מאפשרת חיפוש בקטלוג הגלובלי (Global Catalog), כך שתוכל לאתר חשבונות משתמשים, קבוצות ומדפסות (תרשים 6.8).



תרשים 6.8 תיבת הדו-שיח Find בתוסף התוכנה Active Directory Users And Computers.

כמוצג בתרשים 6.8, ניתן להבחין במספר אזורים ברורים בתיבת הדו-שיח Find: החלון הראשי, כרטיסיית האובייקט, הכרטיסיה Advanced וחלון התוצאות. כרטיסיית האובייקט בתרשים 6.8 היא Users And Groups, Contacts.

הערה שים לב להבדל בין הפקודה Find המתקבלת בחלונות Active Directory לבין הפקודה search המופיעה בתפריט start וכן מתקבלת בתפריט File מתוך הסייר (Windows Explorer).

הפקודה Find מתייחסת לאיתור אובייקטים בספריית Active Directory ואילו הפקודה search מתייחסת לאיתור אובייקטים בסייר, כגון: קבצים ותיקיות. ניתן מחלון search, לבחור גם באיתור אובייקטים בספריית Active Directory, כגון: מדפסות המפורסמות ברשת. אם תבחר לחפש מדפסת, יופיע חלון איתור המציג בשורת הכותרת את Find.

החלון הראשי

החלון הראשי של הכלי Find מכיל ערכת תפריטים, לחצנים ותפריטים נפתחים. אף שרוב האפשרויות מסבירות את עצמן והן מתפקדות בצורה הרגילה המקובלת, התפריטים הנפתחים Find ו-In (תרשים 6.8) הם ייחודיים לתיבת הדו-שיח Find של Active Directory ונידונים ביתר פירוט בהמשך. בנוסף, החלון הראשי כולל שתי כרטיסיות: כרטיסיית האובייקט וכרטיסיית הגדרות מתקדמות, שגם הן נידונות בהמשך פרק זה.

התפריט Find

התפריט Find מכיל את סוג האובייקט אותו ניתן לכלול בחיפוש.

עליך לבחור אחת מהאפשרויות הזמינות לביצוע החיפוש. הבחירה של ברירת המחדל היא Users And Groups, Contacts.

הערה כותרת תיבת הדו-שיח משתנה בהתאם לסוג החיפוש שנבחר מהתפריט הנפתח של Find. לדוגמה, אם Organizational Units נבחר, כותרת תיבת הדו-שיח תהיה Find Organizational Units.

התפריט In

התפריט In, מציין את המיקום בו אתה רוצה לחפש. המיקום יכול להיות Active Directory store כולו, Domain מסוים, או יחידה ארגונית. עליך לבחור באחת האפשרויות. ברירת המחדל היא ה-Domain בו אתה נמצא.

הכרטיסיה Users And Groups, Contacts

הכרטיסיה Users And Groups, Contacts נבחרת בעת פתיחת תיבת הדו-שיח Find. הכרטיסיה מכילה את תיבות הטקסט Name ו-Description. שם האובייקט מוקלד בתיבת הטקסט Name, ותיאור האובייקט מוקלד בתיבת הטקסט Description. ניתן להקליד נתונים בכל אחת מתיבות טקסט אלה, או בשתיהן גם יחד. החיפוש מבוסס על שילוב שתיהן. ניתן גם להשתמש בתו-הכללה (Wild Card) כוכבית (*) וסימן שאלה (?) בשתי תיבות הטקסט לביצוע חיפוש.

הכרטיסיה Advanced

הכרטיסיה Advanced כוללת הגדרות חיפוש מתקדמות המשמשות יחד עם כרטיסיית האובייקט או לבד. תוצאת החיפוש מבוססת על שילוב הנתונים בשתי הכרטיסיות. אם לא הוכנסו נתונים כלשהם לתיבות הטקסט בכרטיסיה Users And Groups, Contacts, יתבססו תוצאות החיפוש רק על הנתונים שבכרטיסיה Advanced.

הטבלה להלן מפרטת את השדות שבכרטיסיה Advanced:

שדה	תיאור
Field	רשימת מאפיינים שניתן לחפש בסוג האובייקט שבחרת.
Condition	השיטות הזמינות לחידוד נוסף של חיפוש המאפיין. האפשרויות הן: Starts With (מתחיל עם), Ends With (מסתיים עם), Is (Exactly) (בדיוק), Is Not (אינו), Present (נוכח), או Not Present (אינו נוכח).
Value	הערך עבור התנאי של השדה (מאפיין) בו אתה משתמש לחפש בספריית הרשת. ניתן לחפש אובייקט באמצעות מאפיין של האובייקט רק אם תכניס ערך למאפיין זה. לדוגמה, אם ערך השדה שתבחר עבור **שם פרטי** וערך התנאי הוא Starts With (מתחיל עם), תיבת הטקסט Value תכיל את האות R אם אתה מחפש את כל המשתמשים ששמם הפרטי מתחיל ב-R.
Search Criteria	תיבה זו נותנת רשימה של כל הקריטריונים שהגדרת. לאחר שהגדרת את הקריטריונים של החיפוש בתיבות שדה, תנאי, וערך, לחץ Add (הוסף). הקריטריונים של החיפוש מתוספים לחלון. תוכל להוסיף או לגרוע קריטריונים כדי להרחיב או לצמצם את החיפוש.

חלון תוצאות

חלון התוצאות נפתח בתחתית החלון הראשי ומציג את תוצאות החיפוש לאחר שלחצת על לחצן Find Now, הנמצא בחלון הראשי. ניתן להוסיף או למחוק עמודות מחלון התוצאות באמצעות אפשרות Choose Columns שבתפריט View.

שינוי ערכי מאפיינים ומחיקת אובייקטים

ניתן לשנות את ערכי המאפיינים של אובייקט, כדי לשנות או להוסיף לו נתונים. שינוי אובייקט משנה את ערך המאפיין המשויך לאובייקט.

הערה אין לבלבל בין שינוי ערך מאפיין של אובייקט לבין הוספה, מחיקה, או שינוי אובייקטים או מאפיינים בסכמה. שינויי סכמה הם קבועים ומשוכפלים לכל בקרי ה-domain ביער.

לשינוי ערכי מאפיין, פתח את תוסף התוכנה Active Directory Users And Computers, ובחר אובייקט. לחץ Properties מתפריט Action. בתיבת הדו-שיח Properties, בצע את השינויים הנדרשים לערכי המאפיין. יש לשנות אובייקטים כאשר ערכי המאפיינים משתנים; לדוגמה, שנה אובייקט של משתמש בשינוי השם, המיקום, או הדואר האלקטרוני של אותו משתמש.

לשמירת האבטחה, מחק אובייקטים כאשר אין בהם עוד צורך. למחיקת אובייקטים, פתח את תוסף התוכנה Active Directory Users And Computers, ובחר את האובייקט שברצונך למחוק. לחץ Delete מתפריט Action.

העברת אובייקטים

ניתן להעביר אובייקטים ממקום אחד ב-Active Directory store למקום אחר, כגון מיחידה ארגונית אחת לשנייה, לשקף שינויים בתוך הארגון. יש להעביר אובייקטים ממקום אחד לשני כאשר מתרחשים שינויים ארגוניים או ניהוליים; לדוגמה, עובד עובר ממחלקה אחת לאחרת. להעברת אובייקט, פתח את תוסף התוכנה Active Directory Users And Computers, ובחר את האובייקט שברצונך להעביר. מתפריט Action, לחץ Move ובחר את המקום החדש עבור האובייקט.

תרגיל 6: ניהול אובייקטים של Active Directory

בתרגיל זה, תאתר תחילה אובייקט משתמש שיצרת בתרגיל הקודם, ותעביר את האובייקט למקום חדש.

הליך 1: מציאת חשבון משתמש ב-Domain

בהליך זה תאתר משתמש עם שם פרטי Jane. Jane קודמה וקיבלה תפקיד במחלקת המכירות, כך שיש להעביר את אובייקט המשתמש שלה ליחידה הארגונית של המכירות. ידועים לך שמה הפרטי ורוב הספרות במספר הטלפון שלה.

1. היכנס לשרת Server01 בשם משתמש Administrator עם הסיסמה password.
2. פתח את Active Directory Users And Computers.
3. בחלון Tree, לחץ microsoft.com.
4. פתח את תפריט Action, ולחץ Find.

   תופיע תיבת הדו-שיח Find Users, Contacts, And Groups.
5. ודא שבתיבת הרשימה הנפתחת Find נבחר Users, Contacts, And Groups, ולחץ Find Now. שים לב כיצד מאותרים כל המשתמשים והקבוצות, ללא תלות במיקומם.
6. לחץ Clear All, ולחץ OK, לאשר שברצונך למחוק את תוצאות החיפוש.
7. בתיבת הרשימה הנפתחת, ודא ש-Microsoft domain מופיע.
8. בתיבת הטקסט Name, הקלד **Jane.**
9. בחר בכרטיסיה Advanced.
10. לחץ Field, הצבע על User, ולחץ Telephone Number.

הערה אם Telephone Number **אינו מופיע** ברשימה, לחץ על החץ בתחתית הרשימה כדי לעלעל למטה עד מספר הטלפון.

בתיבה Condition יופיע Starts With.

11. בתיבת הטקסט Value, הקלד **555-12** ולחץ Add.

12. פתח את תפריט View, ולחץ על Choose Columns.

תופיע תיבת דו-שיח Choose Columns.

13. מתיבת Columns Available, לחץ Description, ולחץ Remove.

14. מתיבה Columns Available, עלעל למטה ולחץ X500 Distinguished Name, ולחץ Add.

15. לחץ OK לסגירת תיבת הדו-שיח Choose Columns.

תיבת הדו-שיח Find Users, Contacts, And Groups תציג את Jane Doe אם ערך סוג אובייקט User ושם ייחודי X.500 של:
CN=Users ,CN=Jane Doe ,DC=microsoft ,DC=com.

Distinguished Name מציין שמשתמשת בשם Jane Doe נמצאת במכולה Users בmicrosoft.com -domain.

16. סגור את תיבת הדו-שיח Find Users, Contacts, And Groups.

הליך 2: העברת אובייקט ב-Active Directory Users And Computers

בהליך זה תעביר את אובייקט המשתמש Jane Doe מהמכולה Users למכולה Sales.

1. בתוסף התוכנה Active Directory Users And Computers, לחץ על Users OU בחלון Tree. כל האובייקטים של קבוצת Users and Security מופיעים בחלונית הימנית.
2. לחץ על אובייקט המשתמש Jane Doe שבחלונית הימנית.
3. פתח את תפריט Action, ולחץ על Move. חלון Move יופיע.
4. לחץ על Sales OU ולחץ OK. Jane Doe מועברת מ-Users OU ל- Sales OU.
5. לחץ על Sales OU בחלון Tree. אובייקט המשתמש Jane Doe יופיע בחלונית הימנית.
6. סגור את תוסף התוכנה Active Directory Users And Computers.

בקרת גישה לאובייקטים של Active Directory

Windows 2000 משתמשת במודל אבטחה מכוון-אובייקט כדי ליישם בקרת גישה על כל האובייקטים של Active Directory. מודל אבטחה זה דומה למודל האבטחה בו משתמשת מערכת Windows 2000 ליישום אבטחת NTFS. לכל אובייקט Active Directory יש מציין אבטחה (Security Descriptor) המגדיר למי יש הרשאות גישה ואיזה סוג גישה מורשית. Windows 2000 משתמשת במצייני אבטחה אלה לבקרת גישה לאובייקטים.

להפחתת ההוצאות הניהוליות הכלליות, ניתן לקבץ אובייקטים עם דרישות אבטחה זהות באותה יחידה ארגונית, ואז להקצות הרשאות גישה לכל היחידה הארגונית ולכל האובייקטים ביחידה.

ניהול הרשאות Active Directory

הרשאות Active Directory מספקות אבטחה למשאבים, על ידי מתן שליטה על יכולת הגישה לאובייקטים ומאפייני אובייקטים ועל סוג הגישה המורשית.

אבטחת Active Directory

השתמש בהרשאות Active Directory לקבוע למי יש הרשאות גישה לאובייקט ואת סוג הגישה המורשית. מנהל או בעל האובייקט חייב להקצות הרשאות לאובייקט לפני שמשתמשים יכולים לקבל גישה לאובייקט. Windows 2000 אוגרת רשימת הרשאות גישה של משתמשים, הנקראות ACL, עבור כל אובייקט ב-Active Directory. ACL (Access Control List) של אובייקט הוא רשימה של מי יכול לגשת לאובייקט והפעולות המסוימות שכל משתמש יכול לעשות באובייקט.

ניתן להשתמש בהרשאות להקצות זכויות למשתמש מסוים או קבוצה מסוימת של יחידה ארגונית, היררכיית יחידות ארגוניות, או אובייקט בודד, בלי להקצות הרשאות ניהוליות לשליטה על אובייקטים אחרים של Active Directory.

הרשאות אובייקטים

סוג האובייקט קובע איזה הרשאות תוכל לבחור. ההרשאות משתנות בהתאם לסוג האובייקט. לדוגמה, תוכל לתת הרשאת איפוס סיסמה (Reset Password) לאובייקט של משתמש, אך לא לאובייקט של מחשב.

משתמש יכול להיות חבר במספר רב של קבוצות, כל אחת עם הרשאות שונות המאפשרות רמות גישה שונות לאובייקטים. כשאתה מקצה הרשאה למשתמש לגישה לאובייקט, ומשתמש זה חבר בקבוצה שהוקצתה לה הרשאה שונה לאובייקט זה, הרשאות המשתמש שייושמו תהיינה שילוב הרשאות המשתמש והרשאות הקבוצה. לדוגמה, אם למשתמש הוקצתה הרשאת Write Account Expiration Data (כתיבת נתוני פקיעת החשבון, הנכתבת בצורת Write accountExpires), לחשבונות משתמשים, והוא חבר בקבוצה שלה הרשאת קריאה של נתוני פקיעת החשבון (Read accountExpires), ההרשאה המשפיעה של המשתמש היא קריאה וכתיבה של נתוני פקיעת החשבון.

הערה Deny תמיד מנצח

תוכל להעניק או למנוע הרשאות. הרשאות שנמנעו מקבלות עדיפות על הרשאות שהוענקו למשתמשים וקבוצות. אם תימנע הרשאת גישה ממשתמש לאובייקט, למשתמש לא תהיה הרשאה זו, אף אם תאפשר הרשאה זו לקבוצה שבה המשתמש חבר. השתמש באפשרות מניעת הרשאה רק כאשר נדרש למנוע הרשאה ממשתמש מסוים שהוא חבר בקבוצה שיש לה ההרשאות.

הערה **ודא תמיד שלכל אובייקט יש לפחות משתמש אחד עם הרשאת Full Control (שליטה מלאה). אם לא תעשה כן, תיתכן תוצאה של אי יכולת גישה לאובייקטים מסוימים על ידי אדם שמשתמש בתוסף התוכנה Active Directory Users And Computers - אפילו Administrator.**

הקצאת הרשאות Active Directory

תוכל להשתמש בתוסף התוכנה Active Directory Users And Computers להגדרת הרשאות לאובייקטים והגדרת מאפייני אובייקטים. הכרטיסיה Security בתיבת הדו-שיח Properties של האובייקט מאפשרת הקצאת הרשאות.

הערה אם אינך רואה את כרטיסיית האבטחה של אובייקט, לחץ Advanced Features מתפריט View.

הרשאות סטנדרטיות מספיקות עבור רוב המטלות הניהוליות. אולם, ייתכן שתצטרך לעיין בהרשאות המיוחדות. לעיון בהרשאות מיוחדות, לחץ Advanced. בכרטיסיה Permissions, לחץ על הרישום שברצונך לעיין, ולחץ View\Edit. לעיון בהרשאות עבור מאפיינים מסוימים, לחץ על כרטיסיית Properties של תיבת הדו-שיח Permission Entry.

הערה הימנע מהקצאת הרשאות עבור מאפיינים ייחודיים של אובייקטים, כיון שזה יסבך את ניהול המערכת. עלולות להיווצר שגיאות, כגון הפיכת אובייקטים של Active Directory לבלתי נראים.

ירושת הרשאות

בדומה לירושת הרשאות (Permissions Inheritance) אחרות במערכת Windows 2000, הורשת הרשאות בשירותי Active Directory ממזערת את מספר הפעמים שנדרש להקצות הרשאות לאובייקטים. בעת הקצאת הרשאות, ניתן להחיל הרשאות על תת-אובייקטים (צאצאי אובייקטים), תכונה הגורמת להתרבות ההרשאות לכל צאצאי האובייקטים של אובייקט נתון. תכונה זו מכונה הורשת הרשאות.

תוכל למנוע ירושת הרשאות, כך שאובייקט צאצא לא יירש הרשאות מאובייקט הורה, על ידי הסרת בחירה מתיבת הסימון Allow Inheritable Permissions From Parent To Propagate To This Object (הרשה להרשאות בנות-ירושה להתרבות עבור אובייקט זה). כאשר אתה מונע ירושה, רק הרשאות שתקצה במפורש לאובייקט יחולו. השתמש בכרטיסיית האבטחה בתיבת הדו-שיח Properties למניעת ירושת הרשאות.

כאשר אתה מסיר את הבחירה מתיבת הסימון למניעת ירושת הרשאות, Windows 2000 Server מציגה לפניך תיבה עם שתי אפשרויות:

- ❖ העתקת הרשאות שהורשו בעבר לאובייקט. ההרשאות המפורשות החדשות לאובייקט הן העתקים של ההרשאות שירש בעבר מאובייקט ההורה שלו. עתה, בהתאם לצרכיך, ניתן לבצע כל שינוי נדרש להרשאות.
- ❖ הסרת הרשאות שהורשו בעבר מאובייקט. Windows 2000 תסיר כל הרשאה שהועברה בירושה בעבר. לאובייקט לא יהיו כל הרשאות. עתה, בהתאם לצרכיך, תוכל להקצות כל הרשאה שהיא לאובייקט.

האצלת סמכות ניהולית על אובייקט

ניתן להאציל (Delegate) למשתמשים סמכות ניהולית (Administrative control) על אובייקט כך שיוכלו לבצע מטלות ניהוליות (Administrative tasks) על האובייקט. ישנן דרכים שונות להאצלת סמכות. לאחר שהחלטת למי להאציל את הסמכות, השתמש באשף Delegation Of Control להאצלת סמכויות אובייקט.

האצלת סמכויות מקלה על תפקידו של מנהל הרשת.

ניתן להאציל סמכות ניהולית על אובייקט, על ידי הקצאת הרשאות על האובייקט כדי לאפשר למשתמשים או קבוצות משתמשים לנהל אובייקטים. מנהל יכול להאציל את סוגי הסמכויות הבאים:

- ❖ הקצאת הרשאות לקבוצה או משתמש ליצירה או שינוי אובייקטים ביחידה ארגונית מסוימת.
- ❖ הקצאת הרשאות למשתמש או קבוצה לשינוי זכויות מסוימות עבור מאפייני אובייקט, כגון הקצאת הרשאה לאיפוס סיסמאות בחשבון אובייקט משתמש.

כיון שמעקב הרשאות ברמת היחידה הארגונית קל יותר מאשר מעקב הרשאות על אובייקטים או מאפייני אובייקטים, השיטה הנפוצה ביותר להאציל סמכויות היא הקצאת הרשאות ברמת היחידה הארגונית. הקצאת הרשאות ברמת היחידה הארגונית מאפשרת האצלת סמכויות ניהול עבור האובייקטים הנכללים ביחידה הארגונית. השתמש באשף Delegation Of Control להקצאת הרשאות ברמת היחידה הארגונית (OU).

לדוגמה, תוכל להאציל סמכות ניהולית על ידי הקצאת הרשאה של Full Control על יחידה ארגונית ל-administrator המתאים, רק בתוך Domain הסמכויות שלו. על ידי האצלת סמכות ניהולית על היחידה הארגונית ל-Administrator (מנהל), ניתן למנוע ריכוזיות פעולות ניהוליות ונושאים. בכך מופחת זמן הניהול שלך והעלויות על ידי העברת סמכות ניהולית קרוב יותר לנקודת היישום שלה.

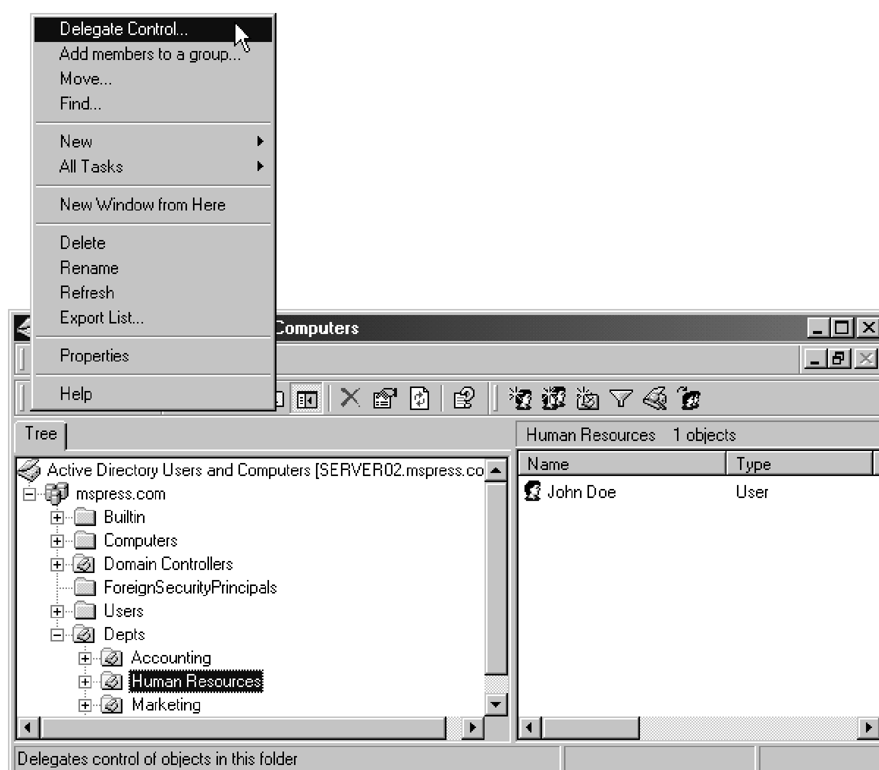
להאצלת סמכויות ניהוליות, היעזר בהנחיות הבאות:

- הקצה סמכות ברמת היחידה הארגונית בכל מקום שמתאפשר. הקצאת סמכות ברמת היחידה הארגונית מאפשר מעקב קל יותר אחר ההרשאות. מעקב אחר הרשאות הוא מסובך יותר עבור אובייקטים ומאפייני אובייקטים.
- השתמש באשף Delegation Of Control. האשף מקצה הרשאות למספר אובייקטים, כולל אובייקטים של יחידות ארגוניות ואובייקטים מובנים אחרים כגון אובייקט של משתמשים ואובייקט של תת-רשת. אובייקט תת-רשת הוא חלק מתוסף התוכנה Active Directory Sites And Services. האשף מפשט את הליך הקצאת ההרשאות לאובייקט, על ידי כך שהוא מוליך אותך צעד אחר צעד.
- עקוב אחר הקצאות האצלת הסמכויות. מעקב אחר ההאצלה מאפשר לתחזק רשומות, כדי לבחון בקלות הגדרות אבטחה.
- היצמד לדרישות עסקיות. היצמד להנחיות הארגון להאצלת סמכויות.

אשף Delegation Of Control

אשף Delegation Of Control מוליך אותך דרך שלבי הקצאת הרשאות ברמת היחידה הארגונית. להרשאות ייחודיות יותר, יש להקצות הרשאות ידנית.

כדי להשתמש באשף Delegation Of Control, פתח את תוסף התוכנה Active Directory Users And Computers, ובחר את היחידה הארגונית שעליה אתה רוצה להאציל סמכויות. בתפריט Action, לחץ על Delegate Control, כדי להתחיל את פעולת האשף (תרשים 6.9).



תרשים 6.9 ניווט באשף Delegate Control.

הנחיות לניהול Active Directory Services

הרשימה הבאה היא אוסף הנחיות לניהול הטוב ביותר של Active Directory Services:

- בארגונים גדולים יותר, תאם את מבנה Active Directory שלך עם מנהלים אחרים. תוכל להעביר אובייקטים מאוחר יותר, אך זה עלול ליצור עבודה נוספת.
- בעת יצירת אובייקטים של Active Directory, כגון Users, השלם את כל המאפיינים החשובים לארגון שלך. השלמת המאפיינים מספקת גמישות גדולה יותר בעת חיפוש אובייקטים.
- השתמש במניעת הרשאות (Deny Permission) בצמצום. אם תקצה הרשאות כנדרש, לא אמור להיות צורך במניעת הרשאות. ברוב המקרים, מניעת הרשאות מעידה על שגיאות שנעשו בעת הקצאת חברות (membership) בקבוצה.

* ודא תמיד שלפחות למשתמש אחד יש הרשאת Full Control עבור כל אובייקט Active Directory. אם לא תעשה כן, ייתכן שאובייקטים מסוימים יהיו בלתי נגישים.
* ודא שמשתמשים מואצלים (Delegated) אכן לוקחים אחריות, ושהם יישאו בתוצאות ויהיו מחויבים במתן דין וחשבון. לא תרוויח מאומה אם תאציל סמכויות ניהוליות בלי שהבטחת נשיאה באחריות עתידית. בסופו של דבר, כמנהל, אתה זה הנושא באחריות על כל השינויים שנעשו. אם המשתמשים להם האצלת סמכויות אינם מבצעים את המטלות הניהוליות שלהם, יהיה עליך לשאת באחריות לכישלונם.
* הדרך משתמשים בעלי סמכויות על אובייקטים. ודא שמשתמשים שלהם האצלת סמכויות, מבינים את מחויבותם ויודעים לבצע את המטלות הניהוליות שלהם.

סיכום שיעור

לאחר התקנת שירותי Active Directory, תוכל ליצור ולנהל את האובייקטים שבתוך ספריית הרשת. לפני הוספת אובייקטים לשירותי Active Directory, עליך ליצור יחידות ארגוניות שיכילו אובייקטים אלה. תוכל ליצור יחידות ארגוניות ברמת הdomain-, ברמה שמתחת ל-DCs, או בתוך יחידה ארגונית אחרת. לשם כך עליך להיות בעל ההרשאות הנדרשות ליצירת יחידות ארגוניות בתוך היחידה הארגונית הקיימת, ה-domain, או DC. להוספת אובייקטים ליחידות ארגוניות, עליך להיות בעל ההרשאות הנדרשות ליצירת אובייקטים בתוך יחידה ארגונית בה אתה רוצה ליצור את האובייקט. הליך ניהול אובייקטים של Active Directory כרוך במספר מטלות שונות, כגון איתור אובייקטים, שינוי ומחיקת אובייקטים, והעברת אובייקטים. מטלות אלו ניתן לבצע באמצעות תוסף התוכנה Active Directory Users And Computers הנמצא בתיקיה Administrative Tools. פן נוסף של ניהול אובייקטים של Active Directory הוא בקרת גישה לאובייקטים של Active Directory. הרשאות Active Directory מספקות אבטחה למשאבים על ידי שליטה במי יהיה בעל גישה לאובייקטים, במאפייני אובייקטים יחידים ובסוג הגישה שתרשה. בנוסף, תוכל להאציל סמכויות ניהול על יחידים, כך שיוכלו לבצע מטלות ניהוליות על אובייקטים.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות לשאלה, עיין בשיעור המתאים ונסה לענות על השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך, מופיעות השאלות באנגלית ואחר כך בעברית.

1. What is Ntdis. dit, and what is its purpose?
2. What is the one SYSVOL location requirement?
3. What is the function of SYSVOL, and what is the one disk requirement for SYSVOL?
4. What is the difference between an attribute and an attribute value? Give examples.
5. What is the difference between modifying an object and modifying the attribute values of an object instance?
6. You want to allow the manager of the sales department to create, modify, and delete only user accounts for sales personnel. How can you accomplish this?
7. What is the global catalog, and what is its purpose?

1. מה הוא Ntdis.dit ומהי מטרתו?
2. מה דרישת המיקום של SYSVOL?
3. מה התפקיד של SYSVOL, ומהי דרישת הדיסק עבור SYSVOL?
4. מה ההבדל בין מאפיין לבין ערך מאפיין? תן דוגמאות.
5. מה ההבדל בין שינוי אובייקט לשינוי ערכי מאפיין של אובייקט?
6. ברצונך לאפשר למנהל מחלקת המכירות ליצור, לשנות ולמחוק רק חשבונות משתמשים עבור כוח אדם של מחלקת המכירות. כיצד תבצע זאת?
7. מה הוא הקטלוג הגלובלי, ומה מטרתו?

פרק 7

ניהול שרת Windows 2000

אודות פרק זה

פרק זה הוא מבוא לניהול Windows 2000 Server. השיעור הראשון דן ב- MMC (**M**icrosoft **M**anagement **C**onsole). מערכת MMC כוללת ממשק משתמש וכלי תצוגה אחיד המאפשר שילוב של כל רכיבי הניהול המבוססים על Windows ועל האינטרנט, לביצוע משימה מסויימת. זהו הכלי העיקרי המשמש לניהול Windows 2000 ומוצרי Microsoft אחרים כגון, מוצרי BackOffice. שאר הפרק מתמקד במטלות הניהול הייחודיות הכרוכות ביישום User Accounts (חשבונות משתמשים), Group Accounts (חשבונות קבוצה), ו-Group Policies (מדיניות קבוצה).

לפני שתתחיל

לביצוע השיעורים בפרק זה, נדרש:

- מחשב בו מערכת Windows 2000 Server מותקנת ופועלת.
- Active Directory Services של Microsoft מותקנים ופועלים.
- השלמת כל התרגילים בפרקים הקודמים.

שיעור 1: MMC -
Microsoft Management Console

אחד מכלי הניהול העיקריים המשמשים לניהול Windows 2000 הוא **M**icrosoft - MMC **M**anagement **C**onsole. MMC מספק שיטה סטנדרטית ליצירה, שמירה ופתיחה של כלי ניהול. הוא מאחד ומפשט מטלות ניהול שגרתיות. MMC אינו מספק פעולות ניהול כשלעצמו, אך הוא הממשק המארח יישומי ניהול הנקראים Snap-Ins (תוספי תוכנה), המשמשים לביצוע מטלת ניהול אחת או יותר.

לאחר שיעור זה, תוכל

- **לתאר את תפקיד ורכיבי** MMC**, כולל תוספי תוכנה ואפשרויות ניהול** MMC console.
- **ליצור** MMC console **מותאם אישית.**

זמן לימוד משוער: 45 דקות

סביבת MMC

Microsoft **M**anagement **C**onsole - MMC הוא ממשק משותף ומרוכז לניהול יישומים. MMC יכול לפעול תחת מערכות ההפעלה Windows 2000, Windows NT 4.0, Windows 98, ו-Windows 95.

MMC כשלעצמו אינו מספקת סביבת ניהול, אך כן מספק סביבה משותפת ל-**Snap-Ins** (תוספי תוכנה), הכלים התומכים בתפקידי הניהול עצמם. סביבת MMC משלבת בין תוספי התוכנה השונים באופן מושלם, גם בין אלה שמקורם בספקים שונים. מנהלים יכולים ליצור כלים הכוללים תוספי תוכנה רבים, ולשמור כלים אלה לשימוש עתידי, או כדי לשתף אותם עם מנהלים אחרים.

MMC מאפשר לבצע את הפעולות הבאות:

- **לבצע את רוב מטלות הניהול באמצעות MMC בלבד** – השימוש בממשק אחד בלבד במקום ממשקים רבים, חוסך זמן.
- **ניהול ממורכז** – ניתן להשתמש ב-MMC לביצוע רוב מטלות הניהול ממחשב אחד.
- **להשתמש ברוב תוספי התוכנה לניהול מרחוק** – לא כל תוספי התוכנה זמינים לניהול מרחוק, ולכן Windows 2000 מנחה אותך באמצעות תיבת דו-שיח, כאשר אתה יכול להשתמש בתוסף תוכנה מסוים לביצוע משימות ניהול מרחוק.
- **בניית MMC console מותאם אישית** – MMC מאפשר יצירת MMC consoles ייעודיים המכילים את כל, או רק חלק מתוספי התוכנה. את ה-MMC consoles הייעודיים האלה ניתן להפיץ לקבוצות תמיכה, לצורך האצלת סמכויות ניהול.

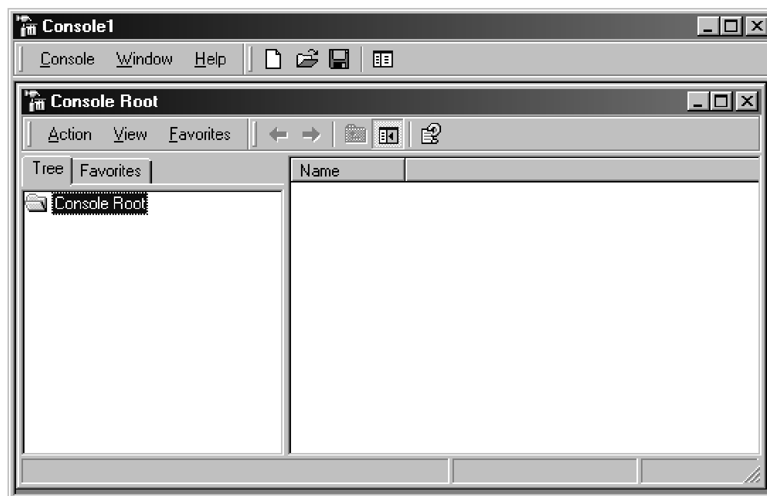
הערה מערכת MMC 1.1 לא תמכה ביותר מתוסף תוכנה אחד, בעוד שמערכת MMC 1.2 שב-

Windows 2000 תומכת בתוספי תוכנה רבים בחלון console בודד.

MMC Window

במבט ראשון, ממשק משתמש MMC נראה ומרגיש דומה מאוד לגירסה של סייר Windows. הרכיבים של MMC console נכללים בחלון MMC. לחלון זה יש מספר תפריטים וסרגל כלים המספקים פקודות לפתיחה, יצירה, ושמירת MM consoles. התפריט וסרגל הכלים מכונים **Main Menu Bar** ו- **Main Toolbar**. בנוסף יש סרגל מצב בתחתית החלון וסרגל תיאור לאורך חלקה העליון של חלונית הפרטים. חלון parent מכיל את חלונות childs, שהם בעצם MMC console.

MMC, כמתואר בתרשים 7.1, ניתן להגדרה כך שיכיל כלי ניהול רבי עוצמה. MMC מתוכנן גם לאפשר מבט ברמה נמוכה יותר, פחות מורכבת, למנהלי רשתות פחות מנוסים.



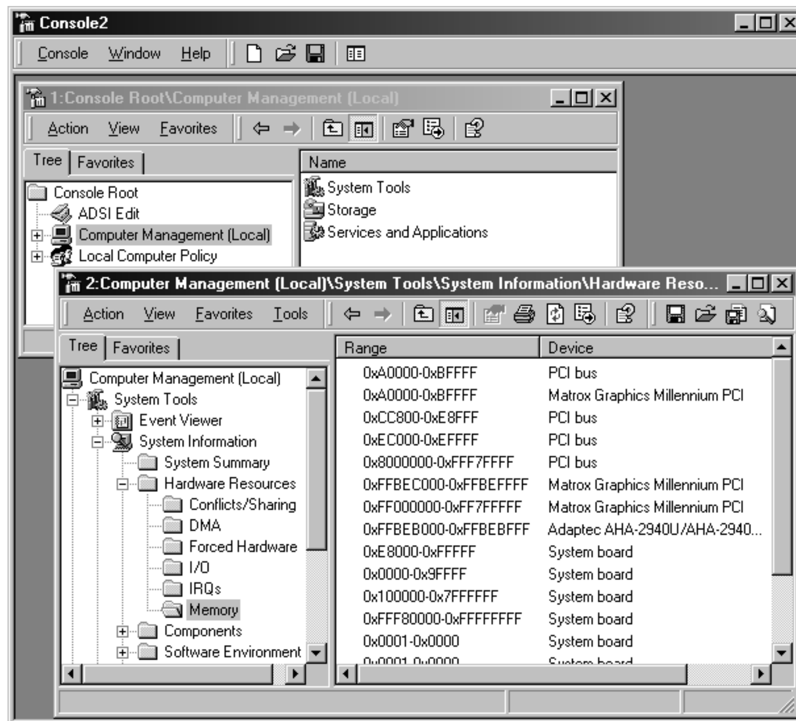
תרשים 7.1 MMC Window.

MMC Consoles

MMC Console הוא ערכה של תוסף תוכנה אחד או יותר. Consoles נשמרים כקבצים בעלי סיומת msc. כל קובץ Console מיוצג על ידי חלון child בממשק MMC. קובץ MMC console מכיל את חלון Tree, המציג את הארגון ההיררכי של תוספי התוכנה הרבים הכלולים בקובץ. כל הגדרות תוספי התוכנה שבחלון console נשמרים ומשוחזרים בעת פתיחת הקובץ, אף אם קובץ msc.*נפתח במחשב אחר ברשת.

Console Window

חלון console, שהוא ממשק לקובץ MMC console, מאפשר מבטים שונים רבים. כל חלון זה כולל סרגל פקודות, חלון Tree (חלונית שמאלית), וחלון פרטים (חלונית ימנית). חלון MMC console שברקע בתרשים 7.2 מציג שלושה תוספי תוכנה, והחלון בקדמה הוא חלון צאצא (Child window) של Snap-In (תוסף) בשם Computer Management.



תרשים 7.2 MMC console המכיל תוספי תוכנה רבים, וחלון צאצא.

סרגל הפקודות כולל תפריטים נפתחים ולחצנים. הטבלה להלן מתארת את תפריטי חלון ממשק הניהול.

תפריט	תיאור
Action	צור, מחק, ושנה פריטים המנוהלים על ידי תוסף התוכנה. תפקידים מסוימים משתנים בהתאם לתוסף התוכנה הפעיל.
View	הגדר את תצוגת תוסף התוכנה.
Favorites	ארגן תוספי תוכנה או צמתים של תוספי תוכנה, או נהל תיקיות המכילות אובייקטים של MMC. רכיבים אלה יופיעו תחת הכרטיסיה Favorites. הכרטיסיה Favorites נמצאת מאחורי הכרטיסיה Tree בתרשימים 7.1 ו- 7.2.

הערה תפריטים נפתחים של רכיבים נוספים **יופיעו** עבור חלק מהאובייקטים **בחלון** Tree. לדוגמה, תרשים 7.2 מציג מצב שבו בעת הבחירה **בצומת** System Information **מחלון** Tree, **יופיע** תפריט נפתח Tools.

חלון Tree, המכונה גם Scope Pane (חלונית ההיקף), מארגן את תוספי התוכנה המהווים חלק מה- MMC console. ארגון זה מאפשר איתור תוספי התוכנה בקלות. רכיבים שתוסיף לחלון Tree יופיעו תחת שורש החלון. חלון Tree מציג את טווח השמות של הכלי ואת הרשימות בתצורת-עץ של כל הצמתים הגלויים, אשר כל אחד מייצג אובייקט לניהול, מטלה, או תצוגה. ייתכן שחלון Tree לא יהיה גלוי בכל המבטים.

כל חלונית פרטים, המכונה גם חלונית התוצאות, מציג את התוצאה של צומת נבחרת בחלון Tree. במקרים רבים, זו היא רשימה של תכולת התיקיה, אך במקרים אחרים, זו היא נקודת מבט ניהולית, היכולה להיות מבוססת אינטרנט או מבוססת בקרת ActiveX.

Types of MMC Consoles

ישנם שני סוגים של MMC console : מותאם אישית (Custom), ומוגדר מראש.

Customized MMC Consoles

תוכל לשלב תוסף תוכנה אחד או יותר, או חלקים של תוספי תוכנה, ליצירת MMC consoles מותאמים אישית (Custom), ולנצלם לריכוז ומיזוג מטלות ניהוליות. MMC console מותאם אישית מאפשר למנהלים לבצע את המטלות הבאות :

- שמירת MMC console מותאם אישית לשימוש חוזר.
- הפצה ושיתוף MMC console מותאם אישית בין מנהלים אחרים.
- שימוש ב-MMC console מותאם אישית מכל מחשב, לרכז ולאחד מטלות ניהוליות.

אף שתוכל להשתמש ברבות מחלונות MMC consoles המוגדרים-מראש למשימות הניהול, לעיתים תרצה ליצור חלונות MMC consoles מותאמים באופן אישי. תוכל לשלב תוספי תוכנה מוגדרים-מראש עם תוספי תוכנה של גוף שלישי (המסופקים על ידי ספקי תוכנה עצמאיים, **I**ndependent **S**oftware **V**endors - ISVs) המבצעים מטלות רלוונטיות, ליצירת מותאמות באופן אישי. יצירת MMC consoles מותאמים באופן אישי מאפשר ביצוע המטלות הניהוליות שלך, על ידי שילוב תוספי תוכנה המשמשים לביצוע מטלות ניהול רגילות. על ידי יצירת MMC consoles מותאמים אישית אינך צריך לעבור בין תוכנות או MMC consoles מוגדרים-מראש, כיון שכל תוספי התוכנה הנדרשים לביצוע עבודתך ימוקמו בחלון Console הניהול האישי (Customized MMC Console).

כברירת מחדל, Windows 2000 שומרת קבצי MMC אישיים בתיקיה My Administrative Tools עם סיומת msc. אם התיקיה My Administrative Tools אינה קיימת, Windows 2000 תיצור אותה. Windows 2000 שומרת את תכולת התיקיה My Administrative Tools עבור כל משתמש בנפרד.

הערה למידע נוסף על יצירת MMC consoles, עיין בתקליטור המצורף לספר זה (\chapt07\articles\microsoft management console.doc).

Preconfigured MMC Consoles

בעת התקנת Windows 2000, מותקנות גם MMC consoles מוגדרים-מראש. MMC consoles מכילים תוספי תוכנה נפוצים המשמשים לביצוע מטלות ניהול. לא ניתן לשנות MMC consoles מוגדרים-מראש, ולא ניתן להוסיף להם תוספי תוכנה (Snap-Ins).

MMC consoles מוגדרים-מראש מכילים רק תוסף תוכנה אחד המספק את התפקודיות הנדרשת לביצוע ערכת מטלות ניהול מוגדרת. MMC consoles פועלים ב-User Mode (מצב משתמש), והמשמעות היא שלא ניתן לשנותם, לשמור אותם, או להוסיף להם תוספי תוכנה אחרים. פעולת מצב משתמש ניכרת בהעדר תפריטי MMC console (התפריטים Console, Window ו- Help) ובהעדר אובייקטים של סרגל הכלים של MMC. בנוסף, MMC consoles נוספים לעיתים בעת התקנת רכיבים. לדוגמה, בעת התקנת שירות **D**omain **N**ame **S**ystem (DNS), Windows 2000 מתקינה גם את DNS console.

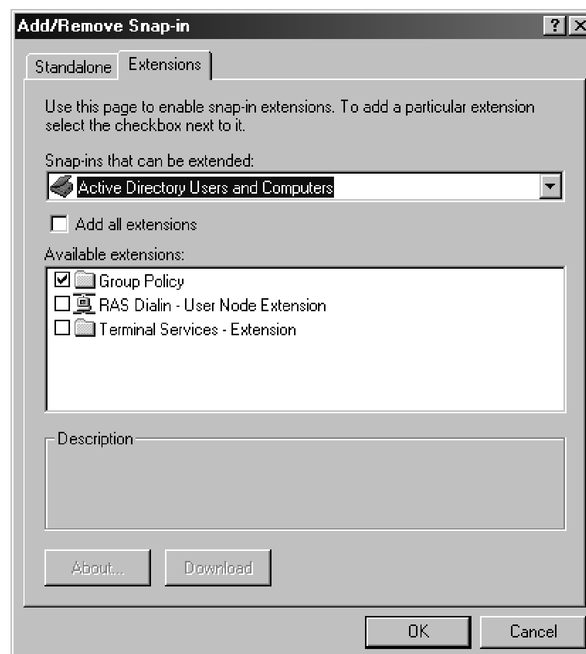
הערה לבחירת MMC consoles מוגדרים מראש, לחץ על לחצן Start, הצבע על Programs, ולחץ על Administrative Tools.

MMC consoles שיותקנו על מחשב משתנים בהתאם למערכת ההפעלה Windows 2000 הפועלת, ורכיבי Windows 2000 המותקנים. למערכות Windows 2000 Server ו-Windows 2000 Professional יש MMC שונים המוגדרים מראש, המופיעים בתפריט Administrative Tools.

ניתן להוסיף MMC consoles מוגדרים-מראש הנכללים ב-Windows 2000 Server גם ל-Windows 2000 Professional, כדי לאפשר ניהול מרחוק של פעולות השרת. דרך נוחה להוספת כל כלי הניהול של Windows 2000 Server היא על ידי הפעלת Adminpak.msi מתקליטור ההתקנה של Windows 2000 Server.

Snap-Ins

כל MMC console בנוי מאוסף כלים קטנים יותר, המכונים Snap-ins. **Snap-Ins** (תוספי תוכנה) הם יישומים שתוכננו לעבוד ב-MMC. תוסף תוכנה אחד מייצג יחידת תפקוד ניהולית אחת. תוסף תוכנה הוא היחידה הקטנה ביותר של הרחבת MMC console. תוסף תוכנה מרחיב את MMC console על ידי הוספת יכולת ניהולית ותפקודיות. ניתן להשתמש בתוספי תוכנה לביצוע מיגוון מטלות ניהול. יש שני סוגים של תוספי תוכנה: Stand-alone ו-Extension (עצמאי והרחבה). תרשים 7.3 מראה את תיבת הדו-שיח Add/Remove Snap-in, שהגישה אליה היא דרך תפריט Console של MMC. שני הסוגים של תוספי התוכנה מתווספים דרך תיבת דו-שיח זו.



תרשים 7.3 תיבת הדו-שיח Add/Remove Snap-in, המראה כיצד תוספי תוכנה מסוג הרחבה, מכוונות מכרטיסיה Extensions.

Stand-Alone Snap-Ins

תוספי תוכנה עצמאיים מכונים לרוב פשוט "תוספי תוכנה". השתמש בתוספי תוכנה עצמאיים לביצוע מטלות ניהול של Windows 2000. כל תוסף תוכנה מאפשר פעולה אחת או ערכת פעולות קשורות. Windows 2000 Server מגיעה עם תוספי תוכנה סטנדרטיים. Windows 2000 Professional כוללת ערכה קטנה יותר של תוספי תוכנה.

Extension Snap-Ins

תוספי תוכנה להרחבה מכונים בדרך כלל Extensions (הרחבות). הם מרחיבים את התפקוד הניהולי של תוסף תוכנה אחר. הרחבות מתוכננות לעבוד עם תוסף תוכנה אחד או יותר, בהתבסס על תפקיד תוסף התוכנה העצמאי. בעת הוספת הרחבה, מציגה Windows 2000 רק הרחבות התואמות לתוסף התוכנה העצמאי. Windows 2000 מניחה את ההרחבות במקום המתאים בתוך תוסף התוכנה העצמאי. כמה תוספי תוכנה, כגון Event Viewer (מציג האירועים), יכולים לשמש גם כתוסף תוכנה וגם כהרחבה.

הרחבות מספקות מיגוון תפקידים. חלקן בעצם מרחיבות את טווח השמות של חלון console. לדוגמה, תוסף תוכנה המספק נתוני מערכת על מחשבים, יוסיף את נתוני המערכת לטווח השמות תחת כל מחשב בטווח השמות. הרחבות אחרות פשוט מרחיבות תפריטי קיצור או אשפים מסוימים.

תוספי תוכנה רבים מספקים תפקוד עצמאי בעודם מרחיבים את התפקודיות של תוספי תוכנה אחרים. לדוגמה, תוסף התוכנה Event Log (יומן אירועים) יקרא את יומני האירועים של המחשבים. אם אובייקט Computer Management קיים באותו console, Event Log מרחיב אוטומטית כל אובייקט Computer Management, ומספק את יומני האירועים למחשב. לחילופין, יומן האירועים יכול לפעול גם במצב עצמאי, ובמקרה כזה הוא אינו מופיע כצומת מתחת לצומת Computer Management.

Console Options

ב-MMC console תמצא תוספי תוכנה המבצעים מטלות מסוימות. אפשרויות MMC console קובעות כיצד הוא פועל. על ידי שימוש באפשרויות MMC console, תוכל ליצור MMC consoles לשימוש administrators אחרים במחשבים שלהם לביצוע מטלות מסוימות. Console Mode קובע את הפעולות העיקריות עבור המשתמש ב-MMC console שנשמר. ישנם שני מצבים עיקריים:

- Author Mode
- User Mode

Author Mode

כאשר אתה שומר MMC consoles ב- Author Mode, אתה מאפשר גישה מלאה לכל הפעולות הכוללות שינוי MMC console. MMC console שנשמר ב- Author Mode מאפשר למשתמשים את הפעילות הבאה:

- הוספה או הסרה של תוספי תוכנה.
- יצירת חלונות חדשים.
- צפייה בכל חלקי חלון Tree.
- שמירת כל MMC consoles.

הערה ברירת המחדל היא שכל MMC consoles החדשים נשמרים במצב Author.

User Mode

אם אתה מתכוון להפיץ MMC console למנהלים אחרים, לרוב תשמור אותו במצב משתמש. בעת הגדרת console למצב משתמש, משתמשים אינם יכולים להוסיף תוספי תוכנה, להסיר תוספי תוכנה, או לשמור את MMC console.

ישנם שלושה מצבי משתמש. כל סוג מאפשר רמת גישה ותפקוד שונה. הטבלה להלן מפרטת מתי להשתמש בכל סוג של מצב משתמש:

סוג מצב משתמש	תיאור
Full Access	מאפשר למשתמשים לנווט בין תוספי תוכנה, לפתוח חלונות חדשים, ולגשת לכל חלקי חלון Tree.
Limited Access, Multiple Windows	מונע ממשתמשים לפתוח חלונות חדשים, או לגשת לחלק מחלון Tree, אך מאפשר להם לצפות בחלונות רבים ב-console.
Limited Access, Single Window	מונע ממשתמשים לפתוח חלונות חדשים, או לגשת לחלק מחלון Tree, ומאפשר להם לצפות בחלון אחד בלבד ב-console.

תרגיל 1: ניווט ויצירת MMC מותאמת אישית

בתרגיל זה תשתמש באחת מ-MMC consoles הכלולים ב-Windows 2000 Server. לאחר מכן תיצור MMC console מותאם באופן אישי.

הליך 1: שימוש ב-MMC console קיים

בהליך זה, תשתמש ב-MMC consoles המצורפים ל-Windows 2000 Server. בצע תרגיל זה משרת Server01.

1. הכנס ל- Server01 בשם משתמש Administrator ועם הסיסמה password.
2. לחץ Start, הצבע על Programs, הצבע על Administrative Tools ולחץ Event Viewer (מציג האירועים).

   Windows 2000 תציג את Event Viewer console, המאפשר גישה לתוכן קבצי השירות של Events Log (יומן אירועים) במחשב שלך. השתמש ב-Event Viewer לניטור פעולות חומרה ותוכנה שונות.

   שים לב שמספר יומנים מופיעים ברשימה. היומנים שתמיד יופיעו בעת התקנת Windows 2000 Server הם Application Log (יומן יישומים), Security Log (יומן אבטחה), ו-System Log (יומן מערכת). יומנים נוספים יופיעו ככל שיתוספו שירותים. עליך לראות את יומן Directory Services (כיון ששרת Server01 מוגדר להפעיל את שירותי Active Directory), יומן DNS (כיון שהוא מוגדר לפעול כשרת DNS) ואת יומן File Replication Service (שירות שכפול קבצים, כיון ששרת Server01 מפעיל FRS שהוא שירות שכפול קבצים).
3. סגור את Event Viewer Console.

הליך 2:
יצירה והפעלה של MMC console מותאם אישית

בהליך זה, תיצור MMC console, ותשנה אותו ל-MMC console מותאם אישית. console זו ישמש לוודא מתי הופעל המחשב לאחרונה. כמו כן תוסיף תוסף תוכנה עם הרחבות.

1. לחץ Start, ולחץ Run.
2. בתיבת הטקסט Open, הקלד **mmc**, ולחץ OK. MMC יופעל ויציג חלון console ריק.
3. הגדל עד למקסימום את חלון Console, על ידי לחיצה על לחצן Maximize.
4. הגדל עד למקסימום את חלון Console Root, על ידי לחיצה על לחצן Maximize בחלון הצאצא.
5. פתח את תפריט Console, ובחר Options לעיין באפשרויות הנוכחיות המוגדרות. MMC יציג את תיבת הדו-שיח Options.

6. באיזה מצב (Mode) פועלת ה-console?

7. ודא שתיבת הרשימה הנפתחת Console Mode מציגה את מצב Author Mode (מצב כותב), ולחץ OK.

8. פתח את תפריט Console ולחץ Save. תופיע תיבת הדו-שיח Save As.

שים לב שמיקום ברירת המחדל ל-MMC consoles מותאמים אישית הוא התיקיה Administrative Tools. זו ממפה לקבוצת Administrative Tools Program עבור המשתמש הנוכחי. ניתן לראות זאת על ידי לחיצה על החץ מטה שמימין לתיבת הרשימה הנפתחת :Save In.

9. בתיבת הטקסט File Name, הקלד **All Events**, ולחץ Save. שם חלון console שלך יופיע בסרגל הכותרת של MMC.

10. כדי לוודא ש-MMC console נשמר במקום הנכון, פתח את תפריט Console, ולחץ Exit.

11. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על All Events.msc. All Events Console, ששמרת קודם, יופיע.

12. פתח את תפריט Console, ולחץ על Add/remove Snap Ins.

תיבת הדו-שיח Add/Remove Snap-Ins תופיע, כאשר הכרטיסיה Stand-Alone פעילה. שים לב שאין כרגע תוספי תוכנה שנטענו.

13. בתיבת הדו-שיח Add/remove Snap Ins, לחץ Add.

תופיע תיבת הדו-שיח Add Stand Alone Snap-In.

14. בתיבת הדו-שיח Add Stand Alone Snap-In, גלול כלפי מטה, בחר את Event Viewer ולחץ Add. תופיע תיבת דו-שיח Select Computer, המאפשרת לך לציין איזה מחשב ברצונך לנהל.

שים לב שתוכל להוסיף Event Viewer למחשב המקומי שעליו אתה עובד, או אם המחשב המקומי הוא חלק מרשת, תוכל להוסיף גם את Event Viewer למחשב מרוחק.

15. בתיבת הדו-שיח Select Computer, ודא שנבחר לחצן אפשרויות Local Computer (המחשב עליו עובד console נוכחי זו), ולחץ Finish.

16. בתיבת הדו-שיח Add Stand-Alone Snap-In, לחץ Close; ובתיבת הדו-שיח Add/Remove Snap-In, לחץ OK.

Event Viewer (Local) יופיע עתה בחלון Tree.

טיפ כדי לראות את שם התיקיה כולו, גרור את הגבול שבין חלוניות ה-console ימינה.

---

17. בחלון Tree של All Event Consoles, הרחב את צומת Event Viewer (Local) ולחץ System. בחלונית התוצאות יופיעו אירועי המערכת האחרונים.

18. לחץ לחיצה כפולה על האירוע האחרון המופיע ברשימה Information בעמודה Type וזו המופיעה ברשימת Eventlog בעמודת Source.

שירות Event Log (יומן אירועים) החל עם הפעלת המערכת. התאריך והשעה מייצגים את המועד בו המערכת שלך החלה לפעול, בקירוב.

19. לחץ OK, כדי לסגור את תיבת הדו-שיח Event Properties.

20. פתח את תפריט Console, ולחץ Exit לסגירת All Events Console.

תופיע תיבת דו-שיח Microsoft Management Console, השואלת אם ברצונך לשמור את ההגדרות של All Events Console.

21. לחץ No.

22. לחץ Start, ולחץ Run.

23. בתיבה Open הקלד **mmc**, ולחץ OK.

24. הגדל עד למקסימום את החלונות Console 1 ו-Console Root.

25. פתח את תפריט Console, ולחץ Add/Remove Snap-In. תופיע תיבת הדו-שיח Add/Remove Snap-In כאשר כרטיסיה Stand-Alone פעילה. עתה תוסיף תוסף תוכנה ל-Console Root.

26. לחץ Add. כל תוספי התוכנה ברשימה המופיעה הם תוספי תוכנה עצמאיים (Stand-Alone).

27. בתיבת הדו-שיח Add Stand-Alone Snap-In, לחץ Computer Management, ולחץ Add. תיבת הדו-שיח Computer Management תופיע.

28. ודא שנבחר לחצן אפשרויות Local Computer (המחשב עליו עובד Console נוכחי זה), ולחץ Finish.

29. לחץ Close. ברשימת תוספי התוכנה שהתוספו יופיע Computer Management.

30. בתיבת הדו-שיח Add/Remove Snap-In, לחץ OK.

תוסף התוכנה Computer Management יופיע תחת Console Root.

31. הרחב את צומת Computer Management, בחן את הפעולות הזמינות, והרחב את צומת System Tools.

הערה אין להשתמש בכלי כלשהו בשלב זה.

שים לב שמספר הרחבות זמינות, כולל Device Manager (מנהל התקנים) ו-System Information (נתוני מערכת). ניתן להגביל את רמת התפקוד של תוסף תוכנה על ידי הסרת הרחבות.

32. פתח את תפריט Console, ולחץ על Add/Remove Snap-In.

תיבת הדו-שיח Add/Remove Snap-In תופיע.

33. לחץ Computer Management (Local), ובחר בכרטיסיה Extensions.

רשימת הרחבות זמינות, הנמצאות בתוסף התוכנה Computer Management תופיע.

34. הסר סימון מתיבת הסימון Add All Extensions, גלול את הרשימה והסר סימון מתיבת הסימון System Information Extension.

35. לחץ OK. חלון Console יופיע.

36. הרחב את Computer Management והרחב את System Tools כדי לודא ש-Device Manager ו-System Information הוסרו.

הערה אין להשתמש בכלי כלשהו בשלב זה.

---

37. פתח את תפריט Console, ולחץ על Options. תיבת הדו-שיח Options תיפתח.

38. מתיבת הרשימה הנפתחת Console Mode, בחר User Mode - Limited Access בחלון בודד.

39. לחץ על תיבת סימון Do Not Save Changes To This Console, ולחץ OK.

40. סגור את חלון Console. MMC תציג הודעה המנחה לאישור שמירת הגדרות ה-Console.

41. לחץ Yes. תיבת הדו-שיח Save As תופיע.

42. בתיבת הטקסט File Name הקלד **ComputerMgmt Restricted**, ולחץ Save.

43. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ ComputerMgmt Restricted. שים לב שה-MMC console המותאם אישית נפתח בחלון בודד.

44. סגור את ה-MMC console המותאם אישית. שים לב שתיבת ההודעות Save This Console אינה מופיעה.

סיכום שיעור

אחד מכלי הניהול העיקריים המשמשים לניהול Windows 2000 Server הוא MMC, המספק שיטה סטנדרטית ליצירה, שמירה, ופתיחת כלי הניהול. בכלים אלה, הנקראים MMC Consoles, נשמרים אחד או יותר תוספי תוכנה, שהם יישומי ניהול המשמשים לביצוע מטלות ניהוליות. כברירת מחדל, Windows 2000 שומרת קבצי MMC consoles מותאמים באופן אישי (Custom) עם סיומת msc בתיקיה Administrative Tools. לכל MMC console יש חלון Tree, המציג את הארגון ההיררכי של תוספי התוכנה שמכיל ה-MMC console, וחלונית פרטים, המספקת רשימה של תכולת תוסף התוכנה הפעיל. יש שני סוגים של תוספי תוכנה: Standalone ו-Extension. תוסף תוכנה עצמאי מספק פעולה אחת או ערכת פעולות קרובות. תוסף תוכנה מורחב מוסיף פעולות ניהוליות לתוסף תוכנה עצמאי. כל MMC Console יכול להיות באחת משתי התצורות: User Mode או Author Mode. מצב משתמש מונע מאחרים הוספה או הסרת תוספי תוכנה ל-Console או שמירת ה-Console. מצב Author מאפשר גישה מלאה לכל פעולות MMC. ניתן ליצור MMC Consoles אישיים ולהפיצם למשתמשים אחרים ברשת.

שיעור 2:
ניהול חשבונות משתמשים

יש ליצור חשבונות משתמשים כדי לאפשר להם להתחבר ל-domain ולגשת למשאבי הרשת, או להתחבר למחשב לקבלת גישה למשאבי המחשב. **User Account** (חשבון משתמש), מכיל את נתוניו הייחודיים של משתמש. זו היא רשומה המגדירה משתמש ל-Windows 2000. היא כוללת את שם המשתמש וסיסמתו אם נדרש, כדי שיוכל להתחבר, את הקבוצות בהן הוא חבר, ואת הזכויות וההרשאות שיש למשתמש במחשב וברשת לגישה למשאבים. כל אדם המשתמש ברשת בקביעות מקבל חשבון משתמש.

לאחר שיעור זה, תוכל

- לתאר את התפקיד ומטרת חשבון המשתמש.
- לתכנן וליצור חשבונות משתמשים.
- לנהל חשבונות משתמשים, כולל הגדרת מאפייני חשבון.

זמן לימוד משוער: 60 דקות

חשבונות משתמשים ב-Windows 2000

חשבון משתמש (User Account) מאפשר למשתמש להתחבר ל-Domain (תחום) לקבלת גישה למשאבי הרשת, או להתחבר למחשב לקבלת גישה למשאבים במחשב זה. כל אדם המשתמש ברשת בקביעות צריך להיות בעל חשבון משתמש.

Windows 2000 תומכת בשני סוגי חשבונות משתמשים: Domain ו-Local. עם domain user account המשתמש יכול להתחבר ל-domain ולגשת למשאבי הרשת. עם local user account משתמש יכול להתחבר למחשב מסוים ולגשת למשאבים במחשב זה.

Windows 2000 גם מספקת built-in user account, המשמשים לביצוע מטלות ניהוליות או גישה למשאבי הרשת.

Domain User Accounts

Domain User Account מאפשרים למשתמשים להתחבר ל-domain ולגשת למשאבים בכל מקום ברשת. המשתמש מספק את הסיסמה שלו ואת שם המשתמש, בעת ביצוע הליך הכניסה (logon) למערכת. עם מידע זה, Windows 2000 מאמתת את המשתמש ובונה אסימון גישה (Access Token) המכיל נתונים אודות המשתמש והגדרות אבטחה. אסימון הגישה מזהה את המשתמש למחשבים המפעילים Windows 2000,

שלמשאביהם מנסה המשתמש לגשת. Windows 2000 מספקת את אסימון הגישה במשך כל זמן ההתחברות של המשתמש.

אתה יוצר Domain User Account ב-OU (יחידה ארגונית), ב- Active Directory Store, המכונה Directory ב-Domain Controller. ה-DC משכפל את נתוני חשבון המשתמש החדש לכל ה-DCs שב-domain.

לאחר ש-Windows 2000 שכפלה את נתוני המשתמש החדש, כל ה-DCs באותו Domain יכולים לאמת את המשתמש בעת תהליך הכניסה למערכת.

הערה **שכפול נתוני** Domain User Account **לכל ה-**DCs **עלול לארוך מספר דקות. עיקוב זה עלול למנוע התחברות מיידית בעת שימוש ב-** Domain User Account **חדש. שכפול נתוני** Active Directory **באתר** (Intra-Site)**, מתרחש אוטומטית כל חמש דקות.**

Local User Accounts

Local User Accounts מאפשרים למשתמשים להיכנס ולגשת למשאבים הנמצאים במחשב, בו נוצר החשבון בלבד. בעת יצירת Local User Accounts, Windows 2000 יוצרת את החשבון במסד נתוני האבטחה של מחשב זה בלבד. Windows 2000 אינה משכפלת את נתוני חשבון המשתמש המקומי ל-DCs. לאחר שחשבון המשתמש המקומי נוצר, המחשב משתמש במסד נתוני האבטחה המקומי שלו, כדי לאמת את החשבון, ובכך מאפשר למשתמש להיכנס למחשב זה.

Built-In User Accounts

Windows 2000 יוצרת חשבונות הנקראים Built-in Accounts. שני חשבונות משתמשים מובנים שנעשה בהם שימוש רב הם Administrator (מנהל) ו-Guest (אורח). מערכת ההפעלה לא תאפשר מחיקה או ביטול של Built-In User Accounts, אולם, ניתן לשנות את שמם של חשבונות מובנים.

Administrator

השתמש ב-Administrator Built-In Account לניהול תצורת המחשב הכוללת וה-domain, כגון יצירה ושינוי חשבונות משתמשים וקבוצות, ניהול מדיניות אבטחה, יצירת מדפסות, והקצאת הרשאות וזכויות לחשבונות משתמשים לקבלת גישה למשאבים.

אם אתה הוא ה-administrator, עליך ליצור חשבון משתמש שישמש אותך לביצוע מטלות לא ניהוליות. השתמש בחשבון administrator רק בעת ביצוע מטלות ניהול הרשת. לנוחות, השתמש בפקודה runas (הפעל כ...) כדי לפעול עם זכויות רבות יותר בעת התחברות עם חשבון בעל זכויות מופחתות.

לדוגמה, להפעלת MMC כמנהל, בעודך מחובר עם הרשאות משתמש רגילות, הפעל את הפקודה הבאה:

```
runas /user:<domain_name>\<administrator_account> "mmc <console_name>.msc"
```

אם חשבון administrator ב-Domain בשם microsoft.com נקרא Administrator, ניתן להשתמש בפקודה הבאה להפעלת MMC DNS Console כ-Administrator:

```
runas /user:microsoft.com\administrator "mmc dnsmgmt.msc"
```

טיפ שנה את שם החשבון Administrator, להגדלת רמת האבטחה. השתמש בשם שאינו מזהה אותו כחשבון administrator. בכך תקשה על משתמשים שאינם בעלי אישור, לחדור לחשבון זה, כיון שאינם יודעים איזה חשבון משתמש זה. להגברת רמת האבטחה, לאחר שתשנה את שם חשבון ה-administrator, צור חשבון אחר בשם Administrator שאין לו כל זכויות במערכת. בכך יסוכלו ניסיונותיו של פורץ מחשבים (Hacker) להשתמש בשם administrator לגישה למערכת.

Guest

השתמש Guest Built-In User Account כדי לאפשר למשתמשים מזדמנים אפשרות התחברות וגישה מוגבלת למשאבים. לדוגמה, עובד הזקוק לגישה למשאבים לזמן קצר יכול להשתמש בחשבון שכזה.

הערה כברירת מחדל, חשבון Guest אינו פעיל. הפעל חשבון זה רק ברשתות בעלות דרישות אבטחה נמוכה והקצה לו תמיד סיסמה.

תכנון חשבונות משתמשים חדשים

ניתן להקל על הליך יצירת חשבונות משתמשים על ידי תכנון וארגון הנתונים עבור חשבונות המשתמשים. עליך לתכנן את שלושת הנושאים הבאים:

- נוהל מתן השמות לחשבונות משתמשים.
- דרישות לסיסמאות.
- אפשרויות חשבון, כגון שעות התחברות, המחשבים מהם משתמשים יכולים להתחבר, ופקיעת חשבון.

מוסכמות של מתן שמות

מוסכמות של מתן שמות קובעים איך משתמשים מזוהים ב-Domain. נוהל שמות עקבי ואחיד יסייעו לך ולמשתמשים לזכור שמות התחברות ולאתרם ברשימות.

הטבלה שלהלן מתמצתת שיקולים שיש לעשות בעת קביעת מוסכמות למתן שמות.

שיקול	הסבר
שמות משתמשים ייחודיים עבור התחברות	שמות התחברות (logon names) של משתמשים לרשת, חייבים להיות ייחודיים ב-Forest. שמות משתמשים (first and last name) חייבים להיות ייחודיים ביחידה הארגונית בה יצרת Domain User Accounts. Local User Accounts חייבים להיות ייחודיים על המחשב בו יצרת אותם.
מקסימום 20 תווים	שמות התחברות (logon name) של משתמשים יכולים להכיל עד 20 תווים באות גדולה או קטנה; קיבולת השדה גדולה מ-20 תווים, אך Windows 2000 מכירה רק את 20 התווים הראשונים.
תווים לא חוקיים	התווים הבאים אינם חוקיים: " \ / [ ] : ; | = , + * ? < >
שמות התחברות יכולים להיכתב באות גדולה וקטנה, ללא השפעה	ניתן לשלב בין תווים אלפא-נומריים ותווים מיוחדים כדי ליצור זיהוי ייחודי למשתמשים. שמות התחברות משתמשים אינם רגישים לאות גדולה או קטנה, אך Windows 2000 שומרת את צורת הכתיבה.
עובדים עם שמות זהים	אם לשני משתמשים קוראים Avi Cohen, תוכל להשתמש בשם הפרטי ובאות הראשונה של שם המשפחה, בתוספת אותיות נוספות, כדי להבדיל ביניהם. בדוגמה זו, שם התחברות של משתמש אחד יכול להיות Avic והשני יהיה Avico. אפשרות נוספת היא למספר כל שם התחברות, לדוגמה, Avic1, Avic2.
סוג העובד	לעיתים נוח לזהות עובד זמני על פי שם המשתמש שלו. לדוגמה, לזהות עובדים זמניים, תוכל להשתמש ב- T ומקף (T=Temporary - זמני): T-Avic. או שתוכל להשתמש בהערה בסוגריים: Avic (Temp).
מוסכמות מתן שמות לחשבון שירות	שירותי רקע רבים דורשים חשבונות משתמש כדי לפעול. שקול לתת סיומת לשם משתמש עם שם כללי כגון svc עבור שירות או שם סוג שירות כגון exc לחשבון ברקע עבור שירותי Microsoft Exchange.

דרישות מתן סיסמאות

להגנה על הגישה ל-Domain או מחשב מקומי, כל חשבון משתמש צריך להיות עם סיסמה. שקול את ההנחיות הבאות לסיסמאות:

- תמיד הקצה סיסמה לחשבון Administrator, כדי למנוע גישה לא מוסמכת לחשבון.
- קבע האם ה-administrator או המשתמשים ישלטו על הסיסמאות. תוכל להקצות סיסמאות ייחודיות לחשבונות המשתמשים ולמנוע ממשתמשים לשנותם, או שתוכל להרשות למשתמשים להכניס את הסיסמאות של עצמם בפעם הראשונה שהם מתחברים. ברוב המקרים, על המשתמשים לשלוט בסיסמאותיהם.
- השתמש בסיסמאות קשות לניחוש. לדוגמה, הימנע משימוש בסיסמאות עם קשר ברור, כגון שם משפחה של משתמש או תאריך הלידה של ילדיו.
- סיסמה יכולה להיות בעלת 128 תווים; מומלץ על מינימום של שמונה תווים.
- השתמש באותיות גדולות וקטנות, ספרות ותווים חוקיים נוספים אחרים. בטבלה הקודמת יש רשימת תווים לא חוקיים.

הערה להבדיל משמות התחברות, סיסמת חשבון כן רגישה להבדל שבין אותיות קטנות ואותיות גדולות.

אפשרויות חשבון

ניתן לשלוט בזמנים בהם משתמש יוכל להתחבר לרשת ולאלו מחשבים הוא יוכל להתחבר. קבע אם חשבונות משתמשים זמניים צריכים לפקוע. לקביעת אפשרויות חשבונות שקול את הפרטים שלהלן.

שעות התחברות

קבע שעות התחברות, כדי לשלוט על מועדי ההתחברות של משתמש ל-Domain. הגבלת שעות התחברות תגביל את השעות בהן משתמש יוכל להשתמש ברשת. ברירת המחדל של Windows 2000 היא התחברות בכל שעה, ללא הגבלה. אולי תרצה להגביל התחברות לשעות העבודה בלבד. קביעת זמן התחברות מפחית את הזמן שהחשבון פתוח לגישה לא מורשת.

מחשבים מהם משתמשים יכולים להתחבר

קבע מאיזה מחשבים המשתמשים יכולים להתחבר לרשת. ברירת המחדל היא התחברות ל-domain מכל מחשב אחר ב-Domain. לאבטחה, דרוש ממשתמשים להתחבר רק מהמחשב שלהם. בכך תמנע ממשתמשים גישה למידע רגיש המאוחסן במחשבים אחרים.

הערה אם בטלת את NetBIOS over TCP/IP, ‏Windows 2000 אינה יכולה לקבוע מאיזה מחשב התחברת, ולכן לא תוכל להגביל משתמשים למחשבים מסוימים. זאת, מכיון שתכונה זו מגבילה גישה לפי שם מחשב, ולא לפי כתובת MAC - **M**essage **A**uthentication **C**ode.

תוקף חשבון

קבע אם חשבון משתמש צריך לפקוע. אם כן, הגדר תאריך פקיעה (Expiration Date) לחשבון המשתמש כדי לוודא שהחשבון מבוטל כאשר למשתמש כבר לא אמורה להיות גישה לרשת. כהרגל אבטחה טוב, עליך להגדיר חשבונות משתמשים של עובדים זמניים כך שיפקעו עם סיום חוזה העסקתם.

יצירת חשבונות משתמשים

ניתן ליצור שני סוגים של חשבונות משתמשים :

- Domain User Account
- Local User Account

יצירת Domain User Accounts

השתמש בתוסף התוכנה Active Directory Users And Computers ליצירת Domain User Account חדש ל-domain. בעת יצירת Domain User Account, הוא נוצר תמיד ב-DC הראשון הזמין ש-MMC console נתקל בו, ואז החשבון משוכפל בכל ה-DCs ב-Domain.

טיפ תוכל ליצור חשבונות משתמשים רבים במהירות על ידי יצירה והפעלת Scripts (תסריט) דרך **W**indows **S**cript **H**ost - WSH (מארח התסריטים של Windows). למידע אודות WSH, פתח את מערכת העזרה של Windows 2000 Server, ואתר את החלק הדן במיכון מטלות הניהול (Automating Administrative Tasks) בפרק "Windows Script Host".

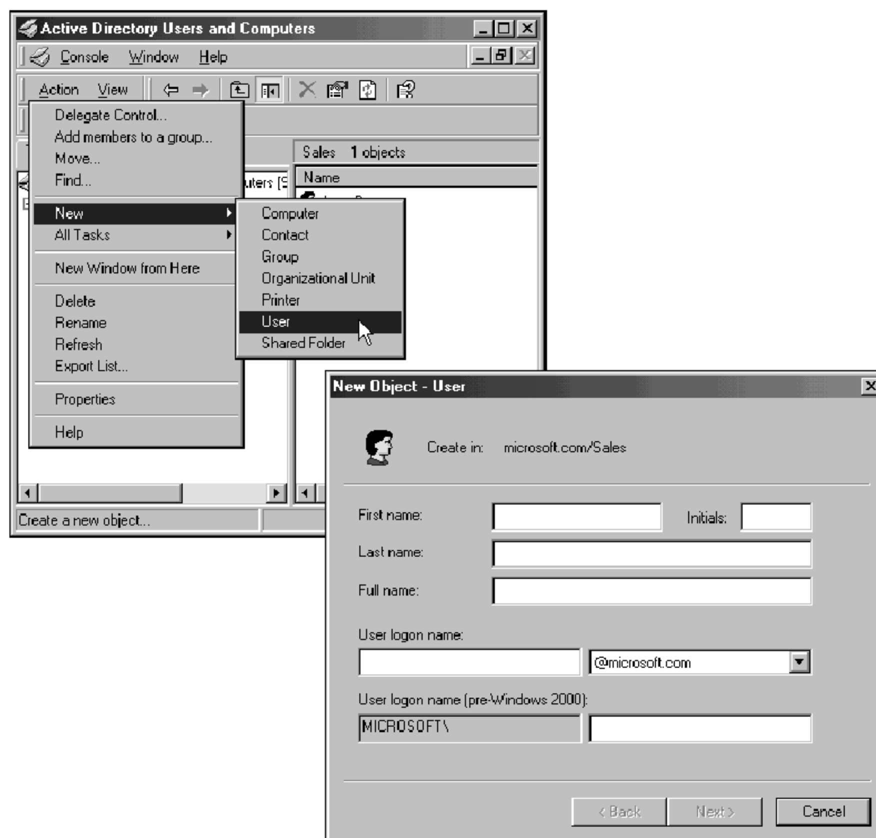
תוסף התוכנה Active Directory Users And Computers

תוסף התוכנה Active Directory Users And Computers מאפשר יצירת Domain User Account (תרשים 7.4).

עליך לבחור יחידה ארגונית (OU) ליצירת החשבון החדש. תוכל ליצור Domain User Account ביחידה הארגונית של ברירת המחדל, Users, או ביחיד/ות ארגוניות שתיצור לשם איחסון חשבונות מסוג זה.

ליצירת Domain User Account, פתח את תוסף התוכנה Active Directory Users And Computers, ובחר ביחידה ארגונית Users. בתפריט Action, הצבע על New והצבע על Users (תרשים 7.4). הכנס את נתוני המשתמש בתיבת הדו-שיח New Object - User.

בעת יצירת Domain User Account חדש, ברירת המחדל של User Logon Name (שם הכניסה למערכת של משתמש) היא ה-Domain בו אתה יוצר את Domain User Account, כמתואר בתרשים 7.4. אולם, ניתן לבחור כל Domain, בו יש לך הרשאה ליצירת Domain User Accounts.



תרשים 7.4 תוסף התוכנה Active Directory Users And Computers ותצוגה איך לנווט לתיבת הדו-שיח New Object - User.

הטבלה הבאה מתארת את אפשרויות Domain User Account :

אפשרות	תיאור
First Name	שמו הפרטי של המשתמש. נדרש לפחות שם זה או שם משפחה.
Last Name	שם משפחתו של המשתמש. נדרש לפחות שם זה או שם פרטי.
Full Name	שמו המלא של המשתמש. Windows 2000 משלימה נתון זה אם הקלדת את שם המשפחה או את השם הפרטי. Windows 2000 מציגה שם זה ב-OU שבה ממוקם חשבון המשתמש ב-Directory.
User Logon Name	שם ההתחברות (הכניסה למערכת, Logon) הייחודי של המשתמש, מבוסס על מוסכמות השמות שלך. זהו שם חובה, וחייב להיות ייחודי ב-Forest.
User Logon Name (pre-Windows 2000)	שם ההתחברות הייחודי של המשתמש להתחברות לקוחות ברמה נמוכה יותר, כגון Windows NT 4.0 , או Windows NT 3.51. זהו שם חובה החייב להיות ייחודי ב-Domain.

הגדרת דרישות סיסמה

בעת הוספת חשבון משתמש חדש, ניתן לקבוע עבורו סיסמה. בתיבת הדו-שיח New Object - User, לחץ Next לפתיחת תיבת דו-שיח נוספת New Object - User. המסך כולל הגדרות סיסמה. בתיבת דו-שיח זו, אתה מגדיר את דרישות הסיסמה עבור Domain User Account. אין חובה לקבוע סיסמה למשתמש. אם לא תקבע עבורו סיסמה, הוא יוכל להתחבר גם ללא סיסמה.

הטבלה הבאה מתארת את האפשרויות לסיסמה :

אפשרות	תיאור
Password	הסיסמה המשמשת לאמת את המשתמש. להגברת האבטחה, יש להקצות סיסמה תמיד. שים לב שאינך רואה את הסיסמה. היא מיוצגת על ידי כוכביות בעת כתיבתה.
Confirm Password	אשר את הסיסמה על ידי הקלדתה שנית לוודא שהקלדת נכון. פעולה זו היא חובה בעת הקצאת סיסמה.
User Must Chang Password at Next Logon	בחר בתיבת סימון זו אם ברצונך שהמשתמש ישנה את סיסמתו בעת ההתחברות הראשונה שלו. בכך מובטח שרק המשתמש יודע את סיסמתו.

אפשרות	תיאור
User Cannot Change Password	בחר בתיבת סימון זו אם יש לך יותר ממשתמש אחד המשתמש באותו Domain User Account (כגון Guest), או כדי לשמור על בקרת סיסמאות חשבונות משתמשים. שימוש בתכונה זו נפוץ עבור בקרת סיסמה לחשבון שירות רקע .
Password Never Expires	בחר בתיבת סימון זו אם הסיסמה אינה צריכה להשתנות לעולם. לדוגמה, ל-domain user account שמטרתו לשמש כתוכנה או כשירות Windows 2000. הגדרת Password Never Expires חזקה יותר ודורסת את ההגדרה User Must Change Password At Next Logon (משתמש חייב לשנות סיסמה בהתחברות הבאה). אם שתי תיבות הסימון נבחרו, Windows 2000 תבטל את הסימון בתיבת הסימון User Must Change Password At Next Logon.
Account Is Disabled	בחר תיבת סימון זו כדי למנוע שימוש בחשבון משתמש זה. לדוגמה, לעובד חדש שטרם התחיל.

הערה דרוש תמיד ממשתמשים חדשים לשנות את סיסמאותיהם בזמן ההתחברות הראשונה. כך תכריח משתמשים להשתמש בסיסמאות הידועות רק להם. להגברת האבטחה ברשתות, צור סיסמאות אקראיות מבוססות ראשי תיבות של השם עבור כל חשבונות המשתמשים על ידי צירוף אותיות וספרות. יצירת סיסמה אקראית מבוססת ראשי תיבות תסייע באבטחת חשבון המשתמש.

תרגיל 2: שינוי תכונות Domain User Account

בתרגיל 5, הליך 1, בפרק הקודם, יצרת שלושה חשבונות משתמשים. בתרגיל זה, תשתמש בתוסף התוכנה Active Directory Users And Computers כדי לטפל במאפייני חשבונות משתמשים של Jane_Doe, John_Smith, ו- Bob_Train. בצע את כל ההליכים בתרגיל משרת Server01.

הליך 1: טיפול בחשבונות משתמשים

בהליך זה, תשנה את מאפייני חשבון המשתמש. תגדיר את שעות ההתחברות, פקיעת החשבון, והגבלות סיסמה עבור מספר חשבונות המשתמשים שיצרת בפרק הקודם. תוסיף חשבונות משתמשים אלה לקבוצת Print Operators כך שהחשבונות יוכלו להתחבר מקומית ל-DC. אחר כך תבחן את הגבלות זמני ההתחברות, הגבלות הסיסמה, ואת הגדרות פקיעת החשבון.

1. היכנס לשרת Server01 בשם משתמש Administrator עם הסיסמה password.

2. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ Active Directory Users And Computers.

תוסף התוכנה Active Directory Users And Computers יופיע.

3. הרחב את הצומת microsoft.com בחלונית השמאלית. חלון Tree יופיע.

4. בחר בתיקיה Users.

5. בחלונית Details, לחץ לחיצה כפולה על רשומת המשתמש Bob Train.

תיבת הדו-שיח Bob Train Properties תופיע והכרטיסיה General תהיה פעילה.

שים לב שבנוסף לשם המשפחה והשם הפרטי, בכרטיסיה General אתה מגדיר מספר מאפייני חשבון משתמש אחרים. ערכי תיבות טקסט כמספר הטלפון בבית ובעבודה, יעילים במיוחד לאיתור משתמשים.

6. בחר בכרטיסיה Account ולחץ Logon Hours.

תופיע תיבת הדו-שיח Logon Hour For Bob Train.

שים לב ש-Bob מורשה להתחבר בכל עת.

7. כדי להגביל את שעות ההתחברות של Bob, לחץ על זמן ההתחלה הראשון שבו ברצונך למנוע מהמשתמש להתחבר, וגרור את הסמן עד לזמן סיום מניעת ההתחברות. להליך נוכחי, מנע התחברות לשלוש השעות הבאות ביום ובתאריך בהם אתה מבצע הליך זה.

חשוב עליך להשלים תרגיל זה במלואו בתוך שלוש שעות, כדי שמגבלת חשבון זה תפעל כיאות. הארך את זמן הגבלת הגישה לזמן בו אתה מתכוון לסיים את התרגיל.

מסגרת מקיפה את כל גושי השעות שנבחרו, והגבלת הזמן מופיעה בחלק השמאלי תחתון של תיבת הדו-שיח Logon Hours For Bob Train.

8. לחץ על לחצן אפשרויות Logon Denied. האזור הממוסגר הוא עתה גוש לבן, המעיד שהמשתמש לא יוכל להתחבר בשעות אלה.

טיפ לבחירת גוש שעות זהה עבור כל ימות השבוע, בשורה המתויגת All, לחץ על הבלוק האפור המייצג את זמן ההתחלה, וגרור את המצביע לזמן הסיום. לבחירת היום כולו, לחץ על הבלוק האפור בעל תג שם היום.

---

9. לחץ OK, כדי לסגור את תיבת הדו-שיח Logon Hours For Bob Train.

10. בתיבת התכונות של Bob Train, לחץ OK להחלת ההגדרות שלך.

11. בחלונית Details לחץ לחיצה כפולה על John Smith.

תיבת הדו-שיח John Smith Properties תופיע, וכרטיסיה General תהיה פעילה.

12. בחר בכרטיסיה Account.
13. מתי החשבון יפקע?
14. בחלק Account Expires, לחץ על לחצן אפשרויות End Of, והגדר תאריך של היום כתאריך.
15. לחץ OK להחיל את השינויים.
16. לחץ על התיקיה Sales בחלון Tree.

החשבון של Jane Doe יופיע בחלונית Details.

17. לחץ לחיצה כפולה על החשבון Jane Doe.

תיבת הדו-שיח Jane Doe Properties תופיע והכרטיסיה General תהיה פעילה.

18. בחר בכרטיסיה Account.
19. בתיבת האפשרויות של Account, לחץ על תיבת סימון User Must Change Password At Next Logon.
20. לחץ OK לסגירת תיבת הדו-שיח Jane Doe Properties.
21. סגור את תוסף התוכנה Active Directory Users And Computers.
22. לחץ Start ולחץ Shut Down. תיבת הדו-שיח Shut Down Windows תופיע.
23. מתיבת הרשימה הנפתחת, בחר Log Off Administrator, ולחץ OK.

Windows 2000 תנתק את חיבור חשבון Administrator, ותציג את תיבת ההודעה Welcome To Windows.

24. לחץ Ctrl+Alt+Delete, והמשך להליך 2.

הליך 2: ניסיון התחברות לשרת Server01 עם חשבון משתמש

בהליך זה, נסה להשתמש בחשבון משתמש Jane Doe (Jane_Doe) להתחבר לשרת Server01.

1. בתיבת הטקסט User Name, הקלד Jane_Doe ללא סיסמה. תיבת ההודעות של ההתחברות מופיעה, ומודיעה שהסיסמה פקעה ויש להחליפה.
2. לחץ OK. תופיע תיבת הדו-שיח Change Password, והסמן בתיבת הטקסט Old Password.
3. לחץ על מקש Tab כיון שלא הוקצתה סיסמה לחשבון Jane_Doe.

4. בתיבת הטקסט New Password ותיבת הטקסט Confirm New Password, הקלד **student**, ולחץ OK. תיבת ההודעות Change Password תופיע, ותודיע שהסיסמה הוחלפה.
5. לחץ OK לסגירת תיבת ההודעות Change Password. האם הצלחת להתחבר בהצלחה? מדוע כן או מדוע לא?
6. לחץ OK לסגירת תיבת ההודעות.

הליך 3: הקצאת התחברות מקומית לחשבונות משתמשים

קיימות מספר שיטות לאפשר למשתמשים קבועים להיכנס באופן מקומי ל-DC. בהליך זה, תוסיף שלושה משתמשים שיצרת בפרק הקודם לקבוצת Print Operators, כיון שלקבוצה יש הרשאה להיכנס ל-DC.

הערה קבוצה היא אוסף של חשבונות משתמשים. קבוצות מפשטות את הניהול בכך שהן מאפשרות הקצאת הרשאות לקבוצת משתמשים ולא הקצאה לכל חשבון משתמש בנפרד. נושא הקבוצות נידון ביתר פירוט בהמשך פרק זה.

---

1. הכנס למערכת בשם משתמש Administrator עם הסיסמה password.
2. פתח את תוסף התוכנה Active Directory Users And Computers, ובחלון Tree, הרחב את היחידה הארגונית Sales.
3. בחלונית Details, לחץ לחיצה כפולה על חשבון משתמש Jane_Doe.

   תיבת הדו-שיח Jane Doe Properties תופיע, כאשר כרטיסיה General פעילה.
4. בחר בכרטיסיה Member Of.
5. לחץ Add. תיבת הדו-שיח Select Groups, תופיע.
6. גלול כלפי מטה את הרשימה בתיבה העליונה, אתר ולחץ על Print Operators.
7. לחץ Add, ולחץ OK, לסגירת תיבת הדו-שיח Select Groups.
8. לחץ OK לסגירת תיבת הדו-שיח של Jane Doe.

   בשלבים הבאים, תשתמש בשיטה פשוטה יותר להוספת חשבונות המשתמשים Bob Train ו-John Smith לקבוצת Print Operators.
9. בחלון Tree, לחץ על התיקיה Users.
10. בחלונית Details, לחץ פעם אחת על Bob Train, לחץ והחזק את מקש Ctrl, ולחץ פעם אחת על John Smith.

11. פתח את תפריט Action, ולחץ Add Members To The Group.

תיבת הדו-שיח Select Group תופיע.

12. גלול כלפי מטה, אתר את Print Operators, ולחץ לחיצה כפולה על רשומה זו.

תופיע תיבת הודעות של Active Directory, המציינת שפעולת Add To Group הושלמה בהצלחה.

13. לחץ OK.

14. סגור את Active Directory Users And Computers, והתנתק מהרשת.

15. נסה להיכנס למערכת בשם משתמש Jane_Doe עם הסיסמה student.

שים לב שעתה תוכל להתחבר מקומית עם חשבון משתמש Jane_Doe.

16. נסה להיכנס למערכת בשם משתמש Bob_Train ללא סיסמה.

שים לב שלא הצלחת להתחבר עקב הגבלת החשבון. בהליך 1, הגבלת את שעות ההתחברות של Bob.

17. נסה להיכנס למערכת בשם משתמש John_Smith ללא סיסמה.

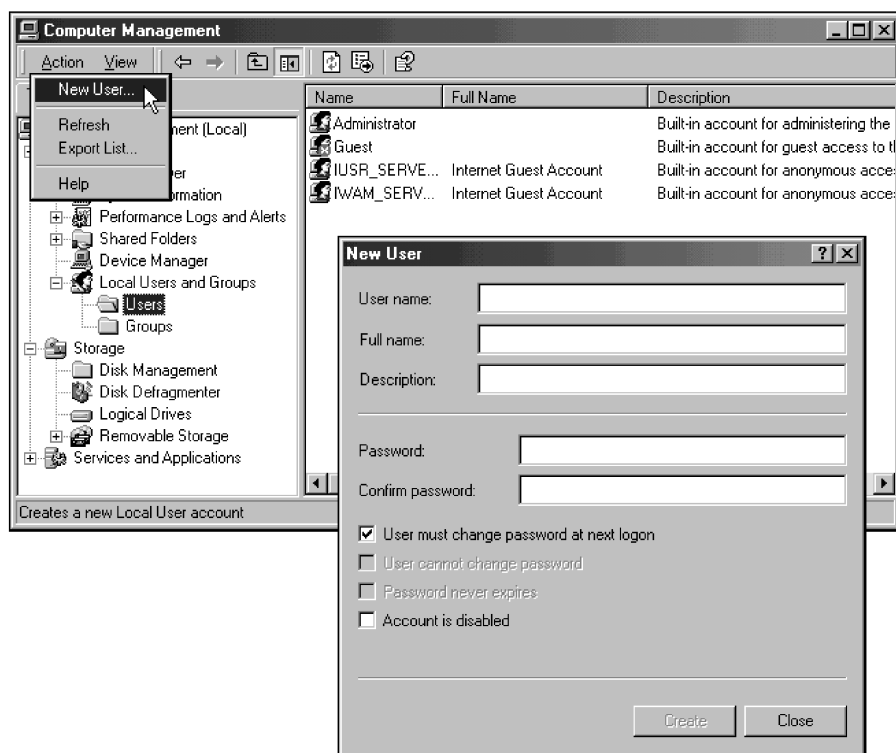
שים לב שניתן להתחבר כחשבון משתמש John_Smith. בהליך 1 הגדרת את פקיעת חשבונו של John לסוף היום. אם תנסה להתחבר כ-John Smith מחר, ההתחברות תיכשל, עקב הגבלת חשבון.

18. התנתק משרת Server01.

יצירת Local User Accounts

Local User Account מאפשר למשתמש להתחבר ולגשת למשאבים רק במחשב בו יצרת את החשבון. השתמש בתוסף התוכנה Local Users And Groups ליצירת חשבונות משתמשים מקומיים (תרשים 7.5).

ניתן ליצור Local User Accounts רק על מחשבים המפעילים Windows 2000 Professional, ושרתים עצמאיים או שרתים-חברים הפועלים תחת Windows 2000 Server. Local User Accounts אינם מאוחסנים ב-Active Directory; הם מאוחסנים במסד נתוני האבטחה המקומי במחשב בו יצרת אותם.



תרשים 7.5 תוסף התוכנה Local Users And Groups בתיבת הדו-שיח New User.

שינוי מאפייני חשבונות משתמשים

בעת יצירת Domain User Account או Local User Account כלשהו, משוייכת אליו ערכת מאפייני ברירת מחדל. Domain User Accounts כוללים יותר תכונות מאשר Local User Accounts. תכונות Local User Account מייצגות תת ערכה של תכונות Domain User Account.

ניתן להשתמש בתכונות המוגדרות עבור Domain User Account כדי לחפש משתמשים ב-Active Directory. מסיבה זו, יש להשתמש בהגדרת תכונות מדויקת של Domain User Accounts. לדוגמה, משתמש יודע את שמו הפרטי והטלפון של אדם, ורוצה למצוא את שם משפחתו. המשתמש יכול להיעזר במספר הטלפון כדי לאתר את שם המשפחה.

יש להגדיר את התכונות הבאות לכל Domain User Account בהתבסס בצרכיו העסקיים של כל משתמש :

- ❖ מאפיינים אישיים, כתובת, טלפונים ופרטי הארגון.
- ❖ מאפייני חשבון.
- ❖ מאפיינים המגדירים את שעות ההתחברות.
- ❖ מאפיינים המגדירים למי ניתן להתחבר.

דרך אחת לשנות Domain User Account היא לפתוח את תוסף התוכנה Active Directory Users And Computers, וללחוץ לחיצה כפולה על אובייקט המשתמש שאת מאפייניו יש לשנות.

דרך אחת לשנות Local User Account היא לפתוח את תוסף התוכנה Computer Management ולבחור Local Users And Groups. לחץ לחיצה כפולה על אובייקט המשתמש אותו נדרש לשנות.

תיבת הדו-שיח Properties

תיבת הדו-שיח Properties עבור כל חשבון משתמש כוללת סדרת כרטיסיות המאפשרות למשתמש להגדיר מספר מאפיינים עבור משתמש מסוים. כל הכרטיסיות המפורטות מטה חלות על Domain User Accounts. רק המאפיינים General, Dial-In, Member Of ו- Profile, חלים גם על Local User Accounts.

כרטיסיות המאפיינים האישיים

כרטיסיות המאפיינים האישיים כוללות את General, Address, Telephones ו-Organization. השלמת הפרטים בכל אחת מכרטיסיות אלו תאפשר למשתמשים ו-administrators לאתר משתמשים אחרים ב-Active Directory Services.

הטבלה הבאה מתארת את הכרטיסיה Personal Properties:

כרטיסיה	תיאור
General	השתמש בכרטיסיה זו לתעד את שם המשתמש, תיאור, מיקום משרד, טלפון, שם דואר אלקטרוני ונתוני עמוד הבית.
Address	השתמש בכרטיסיה זו לתעד את כתובת המשתמש, תא דואר, עיר או מחוז, מיקוד וארץ.
Telephones	השתמש בכרטיסיה זו לתעד את מספרי הטלפון של המשתמש בבית, במשרד, נייד, איתורית, פקס, טלפון IP ולהוסיף הערות.
Organization	השתמש בכרטיסיה זו לתעד את תואר המשתמש, מחלקה ומנהל החברה, ולנתב דוחות.

הכרטיסיה Account

הכרטיסיה Account מאפשרת הגדרת שם ההתחברות (הכניסה למערכת, Logon) של המשתמש, ומאפייני חשבון נוספים לחשבון המשתמש. חלק ממאפיינים אלה הוגדרו כברירת מחדל, בעת שאובייקט חשבון המשתמש נוצר במחסן Active Directory. ניתן לשנות מאפיינים אלה ולהגדיר מאפיינים נוספים.

הכרטיסיה Profile

פרופילי משתמשים יוצרים ומתחזקים באופן אוטומטי את הגדרות שולחן העבודה עבור סביבת העבודה של כל משתמש במחשב המקומי. הכרטיסיה Profile מאפשרת הגדרת נתיב לשיתוף רשת בו יאוחסנו פרופילי המשתמשים. בנוסף, תוכל להקצות תסריט כניסה (Logon Script) להתחברות, ותיקיית בית (Home Folder) לחשבון המשתמש.

הכרטיסיה Published Certificates

Certificate (תעודת הרשאה) היא אוסף נתונים המשמש לאימות ותעבורת נתונים מאובטחת על רשתות לא מאובטחות, כגון האינטרנט. תעודת הרשאה משייכת באופן מאובטח מפתח הצפנה ציבורי ליישות המחזיקה במפתח ההצפנה הפרטי התואם. הכרטיסיה Published Certificate מאפשרת יצירה של רשימת תעודות הרשאה בתקן X.509 עבור חשבונות המשתמשים.

הכרטיסיה Member Of

קבוצות (Groups) משמשות לאיחוד מטלות ניהוליות. לדוגמה, הקצה הרשאת NTFS לקבוצה, ואז הוסף משתמשים לקבוצה. כל חבר בקבוצה מושפע מהקצאת הזכויות. הכרטיסיה Member Of מאפשרת לך לתעד את הקבוצות בהן חבר המשתמש.

הכרטיסיה Dial-In

הכרטיסיה Dial-In מאפשרת שליטה על אופן ההתחברות של משתמש, באמצעות חיוג מאתר מרוחק. לקבלת גישה לרשת, המשתמש מחייג למחשב בו מותקן RAS - **R**emote **A**ccess **S**ervice.

הערה בנוסף להגדרת החיוג והתקנת RAS בשרת אליו מחייג המשתמש, עליך ליצור גם מערך חיבור חיוג לשרת על מחשב הלקוח. צור התחברות בחיוג (Dial-up Connection) באמצעות אשף Network Connection, הנמצא ב-Network Connections שבחלון My Computer.

הטבלה הבאה מתארת את האפשרויות הנדרשות להגדרת אבטחה לחיבור בחיוג:

אפשרות	תיאור
Allow Access	מגדיר אם לאפשר התחברות בחיוג.
Deny Access	מגדיר אם למנוע התחברות בחיוג.
Verify Caller Id	ודא שהמשתמש מתקשר ממספר טלפון מסוים, במידה ושירות מזוהה פעל.
No Callback	מגדיר ששרת RAS לא יחייג חזרה למשתמש. דבר זה מאפשר למשתמש לחייג מכל מספר טלפון. זו היא ברירת המחדל המיועדת לסביבת אבטחה נמוכה, או כאשר מיושמות שיטות אחרות להתחברות בחיוג. כל השיחה היא על חשבון המשתמש.
Set By Caller (Routing And Remote Access Service Only) שיחה על חשבון החברה	מגדיר שהמשתמש יספק את מספר הטלפון אליו יתקשר שרת RAS חזרה. דבר זה מאפשר למשתמש לחייג מכל מספר טלפון, ושרת RAS יתקשר בחזרה למשתמש. ניתן ליצור יומן לנתוני התקשרויות אלה. השתמש בתכונה זו לסביבת אבטחה בינונית.
Allways Callback To	מגדיר ששרת RAS יבצע חיוג חזרה למשתמש. שרת RAS ישתמש במספר הטלפון המוגדר כאן. על המשתמש להיות במספר הטלפון האמור כדי ליצור קשר עם השרת. בכך מופחת הסיכון שאנשים לא מוסמכים יחייגו פנימה, כיון שהמספר מוגדר מראש. השתמש באפשרות זו בסביבות עבודה בעלות רמת אבטחה גבוהה.

הכרטיסיה Object

הכרטיסיה Object מספקת את ה-FQDN - **F**ully **Q**ualified **D**omain **N**ame של האובייקט. היא מספקת גם נתונים נוספים, כגון סיווג אובייקט (Object Class), תאריכי היצירה והשינוי, מספר USN - **U**nique **S**equence **N**umber המקורי, ומספר USN הנוכחי. מספרי USN משמשים למעקב אחר שינויים ב-Active Directory Store.

הכרטיסיה Security

הכרטיסיה Security משמשת להגדרת הרשאות לאובייקט המשתמש במחסן Active Directory. ניתן להקצות או למנוע הרשאות מסוימות לקבוצות או משתמשים בתוך ה-Domain וגם להגדיר הרשאות מתקדמות, וניתן לאפשר או למנוע הורשת הרשאות מאובייקט ההורה לאובייקט המשתמש בעץ Active Directory.

כרטיסיות Terminal Services

כרטיסיות Terminal Services כוללות נתונים על המשתמש, הייחודיים לשירותי המסוף. שירותי מסוף מאפשרים למשתמש להתחבר ממסוף מחשב ולהפעיל עבודה תחת Windows 2000 על המסוף. הנתונים בכרטיסיות שירותי המסוף, כוללים את זמני ההתחברות המורשים של המשתמש, באיזה תנאים, וכיצד מאוחסנות הגדרות שולחן עבודה מסוימות. כרטיסיות שירותי מסוף הן Environment, Sessions, Remote Control ו- Terminal Sessions Profile. להלן פירוט כרטיסיות אלה.

הכרטיסיה Environment

הכרטיסיה Environment מכילה הגדרות ליצירת סביבת העבודה של הלקוח. אם מוגדרת תוכנית התחלה, היא תיפתח אוטומטית בכל פעם שמשתמש יתחבר לשרת מסופים (Terminal Server). זה היישום היחיד הניתן לשימוש על ידי המשתמש. כאשר היישום נסגר, החיבור לשרת המסופים נסגר אף הוא.

תוכל גם להגדיר את חשבון המשתמש, כך ששירותי המסוף יוכלו לחבר כונני לקוחות מקומיים ומדפסות באופן אוטומטי בעת ההתחברות. כאשר הלקוח מתחבר לשרת, המדפסות והכוננים המקומיים מאותרים, ומנהל התקן ההדפסה המתאים מותקן בשרת המסוף. אם מחוברות מספר מדפסות, תוכל להעביר את ברירת המחדל של כל עבודות ההדפסה למדפסת הלקוח הראשית.

הכרטיסיה Sessions

הכרטיסיה Sessions של הרחבת Terminal Services, מספקת הגדרות להגבלת זמן השיח (Session), בהתאם למצבם הנוכחי (פעיל, לא-פעיל, או מנותק). תוכל גם להגדיר איזו פעילות לבצע כאשר Session הגיע לסוף פרק הזמן הקצוב.

הטבלה הבאה מתארת מספר אפשרויות בכרטיסיה Sessions :

הגדרת פסק-זמן	תיאור
End A Disconnected Session	מגדיר את אורך הזמן המירבי לשמירת Session מנותק. ה-Session יאופס, ולא יהיה ניתן לחברו שנית לאחר פקיעת הזמן המוגדר.
Active Session Limit	מגדיר את משך זמן הפעילות המירבי המותר. כאשר מגיעים לזמן הניתוק, ה-Session ינותק, תוך השארת ה-Session במצב פעיל על השרת, או יאופס.
Idle Session Limit	מגדיר את זמן הלא-פעיל המירבי (זמן בו לא מתבצעת פעילות תקשורתית) המורשה לפני ניתוק ה-Session או איפוסו. ה-Session מנותק או מאופס לאחר חלוף הזמן שלא בוצעה פעילות כלשהי בתקשורת.

הכרטיסיה Remote Control

הכרטיסיה Remote Control מאפשרת הגדרת בקרה מרחוק של שירותי מסוף. תוכל לנטר את פעילותו של לקוח המחובר לשרת מסופים על ידי שימוש בשליטה מרחוק משיח אחר. בקרה מרחוק מאפשרת צפייה או שליטה על שיח לקוח. אם תבחר לשלוט באופן פעיל על Client Session (שיח לקוח), תוכל לתת פקודות באמצעות העכבר או מקלדת לתוך השיח. אתה מזהיר לקוח שברצונך לבצע שליטה מרחוק על ה-Session, על ידי שאתה בוחר להציג הודעה ללקוח המבקשת רשות לעיין או להשתתף בו. ניתן לאפשר בקרה מרחוק על חשבון משתמש באמצעות Local Users And Groups (עבור Local Users), או Active Directory Users And Computers (עבור Domain Users).

הערה תכונה זו אינה מאפשרת הפעלת שליטה מרחוק מחיבורים שאינם מסופים. כלים כמו **S**ystem **M**anagement **S**erver (SMS) מספקים שליטה מרחוק לגישה למחשבים ברשת המפעילים מערכות הפעלה Windows.

הכרטיסיה Terminal Services Profile

הכרטיסיה Terminal Services Profile מאפשרת הקצאת פרופיל למשתמש להחלה על Terminal Sessions. לפיכך Administrators יכולים ליצור פרופיל משתמש המתאים לסביבת שירות המסופים. פרופיל שירות המסופים יכול לשמש להגבלת גישה ליישומים על ידי הסרתם מתפריט ההתחלה של המשתמש. Administrators יכולים גם ליצור ולאחסן חיבורי רשת למדפסות ומשאבים אחרים לשימוש ב-Sessions.

תוכל להגדיר נתיב לתיקיה עבור Terminal Sessions. תיקיה זו יכולה להיות תיקיה מקומית, או שיתוף ברשת. תוכל גם להגדיר אם למשתמש יש גישה לשירותי מסוף. אם מבוטלת אפשרות Allow Logon To Terminal Server, המשתמש אינו מורשה להתחבר לשרת מסופים כלשהו.

ניהול חשבונות משתמשים

ניהול חשבונות משתמשים אינו רק יצירת חשבונות משתמש למשתמשים חדשים. הניהול כרוך בשינוי חשבונות משתמשים והגדרת פרופילים ותיקיות. חלק זה מפרט כיצד לבצע מטלות אלה.

ניהול פרופילים של משתמשים

פרופיל משתמש (User Profile) הוא אוסף של תיקיות ונתונים המאחסנים את סביבת העבודה הנוכחית שלך ונתונים אישיים. פרופיל משתמש כולל גם את כל קישורי הרשת המתבצים בעת התחברות למחשב, כגון פריטי תפריט ההתחלה, וכוננים ממופים לשרתי רשת. פרופילי משתמשים שומרים על אחידות בסביבת המחשב, על ידי כך שהם מספקים סביבת עבודה זהה לזו שהיתה לך בפעם האחרונה שהנכנסת למחשב.

Windows 2000 יוצרת פרופיל משתמש מקומי בפעם הראשונה שתיכנס למחשב. לאחר ההתחברות הראשונה, Windows 2000 מאחסנת את פרופיל המשתמש במחשב זה.

פרופילי משתמשים פועלים באופן הבא:

- בעת הכניסה למחשב לקוח הפועל תחת Windows 2000, תמיד תקבל את הגדרות שולחן העבודה הייחודיות שלך והקישורים, ללא תלות בכמות המשתמשים המשתתפים במחשב שלך.
- בפעם הראשונה שתיכנס למחשב לקוח הפועל תחת Windows 2000, Windows 2000 תעתיק את התיקיה Default User המקומית לתיקיה %systemdrive%\Documents and Settings\<**user_logon_name**> (בדרך כלל נמצאת בנתיב C:\Documents and Settings**<User_logon_name**>), כאשר **User_logon_name** הוא שם חשבון המשתמש שלך ב-Windows 2000.
- אם המחשב אליו אתה נכנס שודרג מ-Windows 95 או Windows 98 המאפשרים פרופילים, או מ- Windows NT ל- Windows 2000 Professional, יישאר הפרופיל בתיקיה %systemroot%\profiles, ולא ייווצר בתיקיה Documents and Settings.

- תיקיית פרופיל המשתמש מכילה קבצים ותיקיות רבות לאחסון נתוני משתמש. לדוגמה, התיקיה My Documents היא מקום לאחסון קבצים אישיים. My Documents היא מיקום ברירת המחדל לפקודות Open או Save As (פתיחה או שמירה בשם) של היישומים במערכת. כברירת מחדל, Windows 2000 יוצרת סמל My Documents על שולחן העבודה. כך קל יותר לאתר את מסמכיך האישיים.

הערה **ניתן לשנות את ספריית היעד של** My Documents **על ידי גישה ל-**Properties שבסמל My Documents **על שולחן העבודה.**

- הדרך הפשוטה ביותר לשנות את פרופיל המשתמש שלך היא על ידי שינוי הגדרות שולחן העבודה. לדוגמה, בעת התנתקות מהמחשב לאחר יצירת חיבור רשת חדש, או הוספת קובץ לתיקיה My Documents, Windows 2000 משלבת את השינויים לפרופיל שלך. בפעם הבאה שתיכנס למערכת, חיבור הרשת החדש והקובץ קיימים.

הערה עליך לוודא שמשתמשים שומרים את מסמכיהם ב-My Documents שלהם, **ולא** בספריות הבית שלהם על השרת. Windows 2000 מגדירה את My Documents **באופן אוטומטי, והיא** מיקום ברירת המחדל לשמירת נתוני **יישומים** של Microsoft. **תוך** שימוש בניתוב תיקיות **ותיקיות** לא-מקוונות, נושאים אותם תלמד בהמשך, **ניתן** להגדיר את My Documents כשיתוף ברשת, **ובכך להופכו לזמין למשתמשים בין** אם הם מחוברים **ובין** אם אינם מחוברים לרשת.

Roaming User Profiles

לתמיכה במשתמשים העובדים במחשבים רבים, ניתן להגדיר פרופיל משתמש נודד. **פרופיל נודד** (**R**oaming **U**ser **P**rofile - RUP), הוא פרופיל המוגדר על שרת רשת כך שהוא זמין עבורך מכל מחשב ב-domain אליו תיכנס. כאשר משתמש מתחבר, Windows 2000 מעתיקה את ה-RUP שלו משרת הרשת למחשב הלקוח הפועל תחת Windows 2000 אליו נכנס המשתמש. כתוצאה מכך, המשתמש תמיד מקבל את הגדרות שולחן העבודה האישיות ואת הקישורים שלו. זאת, בניגוד לפרופיל משתמש מקומי, הנמצא אך ורק על מחשב הלקוח הבודד.

כאשר משתמש נכנס, Windows 2000 מחילה את הגדרות ה-Roaming User Profile למחשב זה. בפעם הראשונה שמשתמש נכנס למחשב, Windows 2000 מעתיקה את כל המסמכים למחשב המקומי. מכאן ואילך, כאשר המשתמש נכנס למחשב, Windows 2000 משווה בין קבצי פרופיל המשתמש המאוחסנים מקומית לקבצי הפרופיל הנודד. היא מעתיקה רק את הקבצים שהשתנו מהפעם האחרונה שהמשתמש נכנס למחשב זה. כיון ש-Windows 2000 מעתיקה רק את הקבצים שהשתנו, תהליך ההתחברות קצר יותר.

כאשר משתמש מתנתק, Windows 2000 מעתיקה שינויים שנעשו להעתק המקומי של ה-RUP, חזרה לשרת בו הוא שמור.

יצירת Customized Roaming User Profiles

תוכל גם ליצור ולהקצות Roaming Profile מוגדר מראש, המוקצה לכל חשבונות המשתמשים, וגם להגדיר אותם לקריאה בלבד. תוכל ליצור Customized RUP, על ידי הגדרת סביבת העבודה של שולחן העבודה למשתמש והעתקת הפרופיל האישי למיקום ה-RUP.

השתמש ב-Customized RUP מהסיבות הבאות:

- ❖ לספק למשתמשים סביבת עבודה הנחוצה להם לביצוע עבודתם, ולהסיר קישורים ויישומים שאינם דרושים להם לעבודתם.
- ❖ לספק סביבת שולחן עבודה אחידה למשתמשים רבים בעלי אופי עבודה דומה. משתמשים אלה צורכים משאבי רשת זהים.
- ❖ לפשט איתור תקלות. התמיכה הטכנית תדע בדיוק את בסיס ההגדרות ותוכל לאתר סטייה מהן או תקלה בקלות.

הערה תוכל גם לשנות Local user profiles, אך הדבר אינו מומלץ. הפיכת פרופילים של חשבונות משתמשים מקומיים לפרופילים נודדים אינה יעילה, כיון שהם שוכנים רק על מחשב הלקוח שהמשתמש נכנס אליו.

שימוש ב- Mandatory Profiles

Mandatory Profile הוא Read-Only RUP. כאשר המשתמש מתנתק, Windows 2000 אינה שומרת שינויים כלשהם שהמשתמש יצר בעת עבודתו. בפעם הבאה שהמשתמש ייכנס למחשב כלשהו ב-domain, יופיע לפניו פרופיל זהה לזה שהופיע בפעם הקודמת שהתחבר.

תוכל להקצות Mandatory Profile (נקרא גם פרופיל קבוע) אחד למשתמשים רבים, להם אותן הגדרות שולחן עבודה, למשל כספרי בנקים. מכאן, שניתן לשלוט על ממשק פרופילי משתמשים רבים, מקובץ פרופיל משתמש יחיד.

קובץ נסתר בשם Ntuser.dat מכיל את חלק ההגדרות במערכת Windows 2000 החל על חשבון משתמש בודד, ומכיל את הגדרות סביבת המשתמש, כגון צורת שולחן העבודה. כדי ליצור Mandatory Profile, לקריאה בלבד, יש לשנות את שמו של הקובץ ל-Ntuser.man.

הגדרת Roaming User Profile

בעת הגדרת RUP על שרת, בפעם הבאה שמשתמש ייכנס למחשב ב-Domain, Windows 2000 תעתיק את פרופיל המשתמש המקומי לנתיב ה-RUP בשרת. לאחר שהמשתמש מתחבר, מהפעם השנייה ואילך, ה- RUP יעתיק את הפרופיל מהשרת למחשב.

עליך להגדיר RUP על שרת קבצים שאתה נוהג לגבות לעיתים תכופות, כדי שיהיו לך גיבויים לעת הצורך. לשיפור ביצועי ההתחברות לרשת רבת-תעבורה, התקן את התיקיות המכילות את ה-RUPs על member server, ולא על DC. העתקת ה-RUPs בין מחשבי השרת והלקוח עלולה לצרוך משאבי מערכת רבים, כגון רוחב פס וכוח עיבוד מחשב. אם הפרופילים מותקנים על DC, הדבר עלול לעכב אימות משתמשים.

טיפ לשיפור נוסף של הביצועים וזמינות פרופילים, שקול הגדרת Domain Root Dfs לפרופילי משתמשים והגדרת FRS (שירות שכפול קבצים), כך שהפרופילים משוכפלים לנקודות זמינות רבות ברשת.

להגדרת RUP, עליך ליצור תיקיה משותפת על שרת ולהשתמש בנתיב בפורמט הבא: \\<server>\<share>. השתמש בשם אינטואיטיבי לתיקיה המשותפת, למשל Profiles. בכרטיסיה Profile בתיבת הדו-שיח Properties של חשבון המשתמש, הקלד את הנתיב **\\<server>\share>\<logon_name>** לתיקיה המשותפת בתיבת הטקסט Profile Path.

במקום שם ההתחברות של המשתמש, ניתן להקליד את המשתנה %username%. בעת שימוש במשתנה זה, Windows 2000 מחליפה את המשתנה בשם חשבון המשתמש של ה-RUP, באופן אוטומטי.

הקצאת Customized RUP

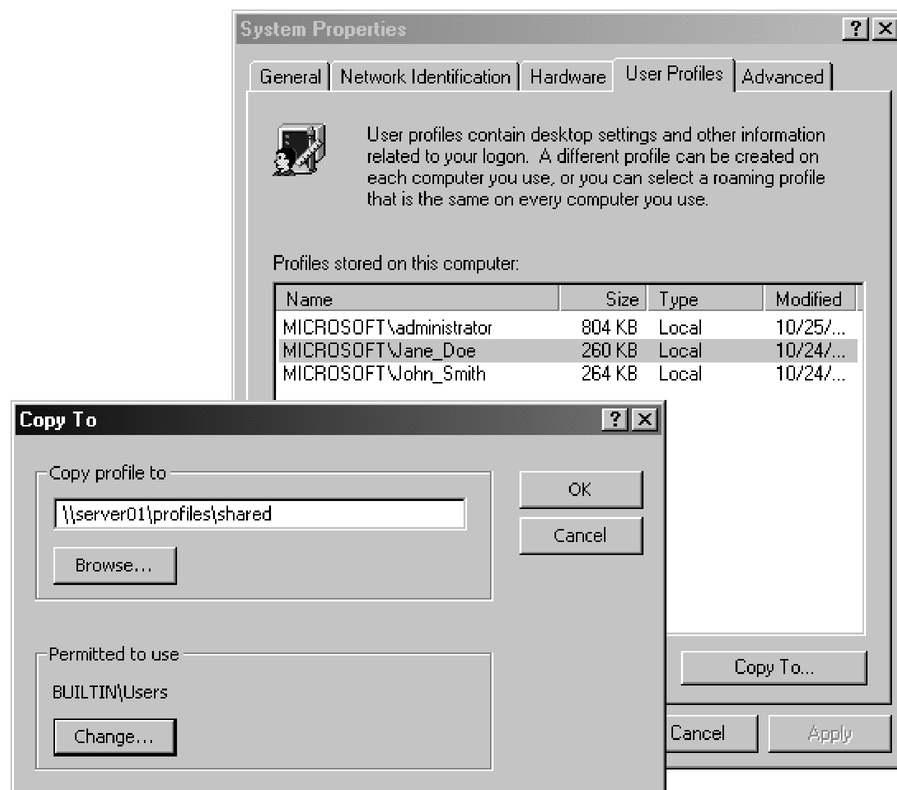
ניתן ליצור RUP מותאם אישית ולהקצותו למשתמשים רבים, כך שתהיינה להם אותן ההגדרות וקישורים כשיתחברו לרשת. לפני שתוכל להקצות RUP ולהתאימו אישית, עליך ליצור User Profile Template (תבנית פרופיל משתמש), המכילה את הגדרות שולחן העבודה המותאמות, כפי שברצונך להקצות למשתמשים. תבנית נוצרת על ידי הגדרת שולחן העבודה בדיוק כפי שאתה רוצה שייראה למשתמשים להם יוקצה הפרופיל. ניתן להשתמש גם בחשבון קיים ולא נדרשים כלים מיוחדים ליצירת התבנית.

לאחר שיצרת User Profile Template (תבנית פרופיל המשתמש), היכנס למערכת כ-administrator והעתק את תבנית פרופיל המשתמש לתיקיה בה נמצאים ה-RUPs בשרת. תיקיה זו חייבת להיות נגישה לכל המשתמשים להם יוקצה פרופיל זה. ניתן להשתמש ביישומון System שבלוח הבקרה להעתקת תבנית הפרופיל למיקום משותף ברשת, כמתואר בתרשים 7.6. שים לב שהפרופיל מוקצה לקבוצה Users המובנית ב-Domain.

להשלמת ההליך, הקצה את הפרופיל למשתמשים המתאימים באמצעות תוסף התוכנה Active Directory Users And Computers. לאחר פתיחת תוסף התוכנה, גש לכרטיסיה Profile בתיבת הדו-שיח Properties Of A User Account, ובתיבת הטקסט Profile Path הקצה נתיב לפרופיל.

כיון ששינוי בתבנית הפרופיל משפיעה על כל המשתמשים להם הוקצה פרופיל זה, עליך להפוך את הפרופיל ל- מנדטורי. כדי להפוך את הפרופיל למנדטורי (קבוע, לקריאה בלבד), שנה את סיומת קובץ Ntuser שבתיקיית הפרופיל בשרת, מ- dat ל- man.

הערה קובץ Ntuser.dat הוא קובץ נסתר. עליך להשתמש בתוכנית השירות attrib משורת הפקודה לשינוי אפיון Hidden, או לאפשר צפייה בקבצים מוסתרים באמצעות סייר Windows.



תרשים 7.6 העתקת תבנית פרופיל Jane_Doe לתת תיקיה (משותפת) של השיתוף \\server01\profiles.

שינוי חשבונות משתמשים

צרכים ושינויים בעסק/ארגון עלולים לעורר צורך לשנות חשבונות משתמשים. לדוגמה, אולי תצטרך לשנות שם חשבון משתמש קיים עבור עובד חדש כך שלעובד זה יהיו אותן הרשאות וגישה לרשת כמו קודמו. שינויים אחרים מבוססים על שינויים אישיים או נתונים אישיים, כגון מניעה, אפשור או מחיקת חשבון משתמש. ייתכן גם שתצטרך לאפס סיסמת משתמש, או לפתוח חשבון משתמש נעול.

הערה ניתן לשנות חשבון משתמש על ידי שינוי אובייקט חשבון המשתמש ב-Active Directory. כדי לבצע בהצלחה את מטלות שינוי חשבונות המשתמשים, יצירת RUPs, והקצאת תיקיות בית, צריכות להיות לך ההרשאות הנדרשות לניהול ה-OU בה שוכנים חשבונות המשתמשים.

מניעה, אפשור, שינוי שם ומחיקת חשבונות משתמשים

להלן שינויים שניתן לעשות לחשבונות משתמשים, ואשר משפיעים על תפקודיות החשבון:

- **מניעה ואפשור חשבון משתמש** – אתה מונע (Disable) חשבון משתמש, כאשר משתמש לא יצטרך חשבון לתקופה ממושכת, אך יצטרך אותו שוב בעתיד. לדוגמה, אם John לקח חופשה למשך חודשיים, אתה אמור להקפיא את חשבונו עם עזיבתו. כאשר יחזור, תוכל לחזור ולאפשר (Re-Enable) את חשבונו, כדי שיוכל להתחבר לרשת שוב.
- **שינוי שם חשבון משתמש** – אתה משנה שם חשבון משתמש, כאשר אתה רוצה לשמור על כל הזכויות, הרשאות, חברויות בקבוצות, ורוב מאפייני חשבון המשתמש, כדי להקצותו למשתמש אחר. לדוגמה, אם יש לחברה מנהל שיווק חדש, שנה את שם החשבון של מנהל השיווק היוצא על ידי שינוי השם הפרטי, שם המשפחה ושם ההתחברות, כך שיתאימו למנהל השיווק החדש.
- **מחיקת חשבון משתמש** – מחק חשבון משתמש, כאשר עובד עזב את החברה, ואינך מתכוון לשנות את שם חשבון המשתמש. על ידי מחיקת חשבונות משתמשים אלה, אין לך חשבונות משתמשים שאינם בשימוש בשירותי Active Directory.

ההליכים למניעה, אפשור, שינוי שם ומחיקת חשבונות משתמשים, דומים עבור Domain או חשבונות Local. עבור Domain User Accounts, השתמש בתוסף התוכנה Active Directory Users And Computers. בחר את חשבון המשתמש, ולחץ על Action בתפריט Action. עבור Local User Accounts, השתמש בהרחבה Local Users And Groups בחלון Tree של תוסף התוכנה Computer Management.

הערה אם חשבון משתמש מאופשר (Enabled), תפריט Action **יציג את פקודת** Disable Account (מנע חשבון). אם חשבון משתמש נמנע, תפריט Action **יציג את פקודת** Enable Account (אפשר חשבון).

איפוס סיסמאות ושחרור חשבונות נעולים

אם משתמש אינו יכול להתחבר ל-domain או למחשב מקומי, ייתכן שתידרש לאפס את סיסמת המשתמש או לשחרר את חשבון המשתמש הנעול. לביצוע מטלות אלה, עליך להיות בעל זכויות ניהול ביחידה הארגונית בה שוכן חשבון המשתמש.

איפוס סיסמאות

אם סיסמת משתמש פוקעת לפני שיוכל לשנותה, או אם משתמש שוכח את סיסמתו, עליך לאפס את הסיסמה.

הערה אין צורך לדעת את הסיסמה הישנה כדי לאפס סיסמה.

לאיפוס סיסמת משתמש, פתח את תוסף התוכנה Active Directory Users And Computers ובחר את אובייקט המשתמש. בתפריט Action, לחץ Reset Password. בתיבת הדו-שיח של Reset Password, הכנס סיסמה ובחר User Must Change Password At Next Logon, כדי לאלץ את המשתמש לשנות את סיסמתו בפעם הבאה שיתחבר.

שחרור חשבון משתמש נעול

מדיניות קבוצה (Group Policy) של Windows 2000 נועלת חשבון משתמש המפר מדיניות זו. לדוגמה, המשתמש ניסה להתחבר ללא הצלחה מספר פעמים רב יותר מאשר מוגדר במדיניות הקבוצה. כאשר חשבון משתמש ננעל, Windows 2000 תציג הודעת שגיאה.

לשחרור חשבון משתמש נעול, פתח את תוסף התוכנה Active Directory Users And Computers, ולחץ לחיצה ימנית על אובייקט המשתמש. לחץ Properties, ובחר בכרטיסיה Account. הסר סימון מתיבת סימון The Account Is Locked Out.

Home Folders

בנוסף לתיקיה My Documents, Windows 2000 מספקת אמצעים ליצירה של תיקיית בית עבור המשתמש. Home Folder (תיקיית בית) היא תיקיה נוספת שניתן לספק למשתמשים, כדי שיוכלו לאחסן בה מסמכים אישיים. לעיתים, ליישומים ישנים יותר, זוהי תיקיית ברירת המחדל לשמירת מסמכים. ניתן לאחסן תיקיית בית על מחשב לקוח, או בתיקיה משותפת בשרת קבצים. כיון שתיקיית בית אינה חלק מה-RUP , גודלה אינו משפיע על תעבורת הרשת בעת ההתחברות (אלא בזמן שמירה ופתיחה של קבצים). ניתן לרכז את כל תיקיות המשתמשים בנקודה אחת בשרת כלשהו ברשת.

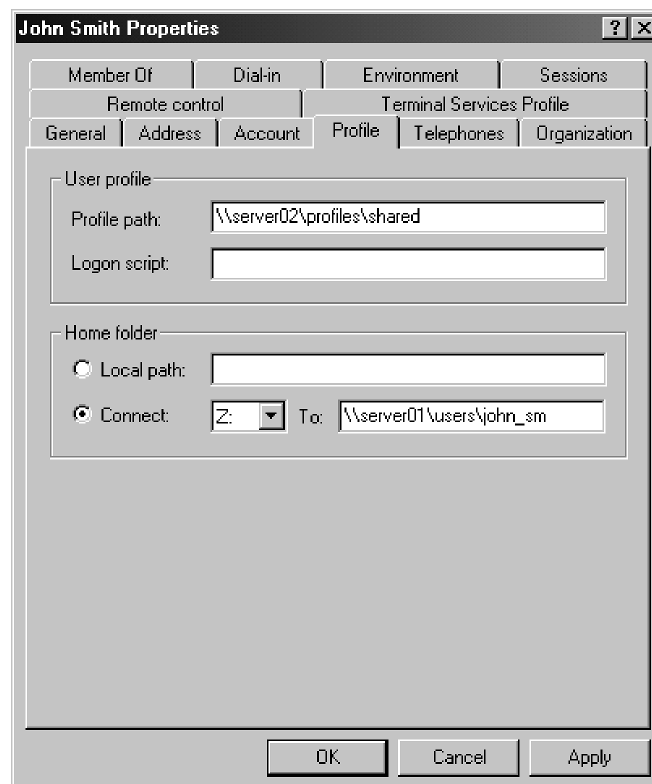
אחסון כל תיקיות הבית בשרת קבצים מספק את היתרונות הבאים:

- משתמשים יכולים לקבל גישה לתיקיות הבית שלהם מכל לקוח ברשת.
- גיבוי וניהול מסמכי משתמשים הוא מרוכז במקום אחד.
- תיקיות הבית נגישות מכל מחשב הפועל תחת מערכת הפעלה כלשהי של Microsoft (כולל MS-DOS, Windows 95, Windows 98 ו- Windows 2000).

הערה עליך לאחסן את תיקיות הבית (home folders) ב-NTFS volume, כדי שתוכל להשתמש בהרשאות NTFS לאבטחת מסמכי משתמשים. אם תאחסן קבצים ב-FAT volume, תוכל להגביל גישה לתיקיות הבית רק באמצעות הרשאות תיקיה משותפת.

ליצירת תיקיית בית על שרת קבצים, יש לבצע את שלוש המטלות הבאות:

- **יצירה ושיתוף של תיקיה** – צור ושתף תיקיה, בה תאחסן את כל תיקיות הבית בשרת. תיקיית הבית עבור כל משתמש תשכון מתחת לתיקיה המשותפת.
- **שינוי הרשאת Full Control** (שליטה מלאה) – עבור התיקיה המשותפת, הסר את הרשאת ברירת המחדל Full Control הניתנת לקבוצה Every One. בכך מובטח שרק משתמשים בעלי Domain User Accounts יהיו בעלי גישה לתיקיה המשותפת.
- **הגדרת נתיב עבור תיקיית הבית** – הגדר את הנתיב לתיקיית הבית של המשתמש בקטע Home Folder בכרטיסיה Profile שבתיבת הדו-שיח Properties של חשבון המשתמש (תרשים 7.7). כיון שתיקיית הבית נמצאת על שרת רשת, לחץ Connect, והגדר אות כונן שתשמש להתחברות. כתוצאה מכך, כאשר המשתמש יתחבר לרשת, אות הכונן שהקצת תופיע בחלון My Computer. בתיבת הטקסט To, יופיע שם UNC בפורמט \\<server>\<share>\<user_logon_name>. ניתן להשתמש במשתנה %username% כשם ההתחברות של המשתמש, כדי ליצור באופן אוטומטי את תיקיית הבית של כל משתמש, כאשר שמה הוא כשם הכניסה למערכת (שם ההתחברות, Logon Name) של אותו משתמש.



תרשים 7.7 הכרטיסיה Profile, כפי שהיא מופיעה בתיבת הדו-שיח Properties של חשבון המשתמש. מוגדרים בה נתיב פרופיל ונתיב תיקיית בית הנגיש דרך הרשת.

הערה אם תשתמש במשתנה %username% כדי לתת שם לתיקיה ב-NTFS volume, המשתמש וקבוצת הניהול המקומית המובנית מקבלים הרשאת NTFS Full Control. כל שאר ההרשאות מוסרות מהתיקיה, כולל אלה עבור קבוצת Everyone Special.

תוכל לשפר את מאפייני תיקיית הבית על ידי הפניית המשתמש מ-My Documents למיקום תיקיית הבית שלו.

תרגיל 3: יצירת Roaming Profile והקצאת תיקיית בית

בתרגיל זה, תשתמש בחשבון משתמש Jane_Doe ליצור פרופיל. לאחר מכן תתחבר כ-Jane Doe ליצירת פרופיל מקומי לחשבון. אחר כך תתחבר כמנהל ותשתמש ביישומון System שבלוח הבקרה, כדי לוודא שהפרופיל של Jane Doe אכן נוצר. בהליך 2, תשתמש בפרופיל Jane_Doe ליצור ולבחון פרופיל נודד מהמחשב השני. בהליך 3, תיצור ותבחן תיקיית בית עבור Jane_Doe.

הליך 1: יצירת תבנית פרופיל משתמש

בהליך זה, תגדיר ותבחן פרופיל משתמש מקומי. תשתמש בשרת Server01 ליצירת תבנית פרופיל משתמש. ככלל, מחשב המפעיל מערכת הפעלה Windows 2000 Professional ישמש ליצירת תבנית פרופיל משתמש. אולם, ההנחה כאן היא שאתה מפעיל Windows 2000 Server רק כדי להשלים את ההליכים המפורטים.

1. אם אתה מחובר בשרת Server01, התנתק.
2. התחבר ל-Domain בשם microsoft.com בשם משתמש Jane_Doe עם הסיסמה student.

   אם זו הפעם הראשונה שהתחברת עם חשבון Jane_Doe, ייווצר עבורו פרופיל משתמש מקומי עם הגדרות ברירת מחדל. פרופיל זה של Jane_Doe ישמש, בתרגיל, כתבנית פרופיל עבור חשבונות אחרים.

3. לחץ לחיצה כפולה על סמל My Computer בשולחן העבודה. חלון My Computer יופיע.
4. לחץ וגרור את סמל הדיסק המקומי (:C) לשולחן העבודה.

   תופיע תיבת הודעות של קיצור דרך, המציינת שלא ניתן להעתיק פריט זה או להזיזו, אך כן ניתן ליצור קצור דרך.

5. לחץ Yes ליצירת קיצור דרך לכונן :C.
6. סגור את חלון My Computer.
7. לחץ Start, הצבע על Settings, לחץ על Control Panel, ולחץ לחיצה כפולה על Display. תיבת הדו-שיח Display Properties תופיע.
8. בחר בכרטיסיה Appearance. שים לב לצבעים הנוכחיים.
9. בתיבה Scheme, בחר ערכת צבע שונה, ולחץ OK. שולחן העבודה ישתנה לפי ערכת הצבע החדשה.

10. סגור את לוח הבקרה.

11. התנתק כ-Jane_Doe, וחזור והיכנס בשם משתמש Administrator עם הסיסמה password.

12. לחץ Start, הצבע על Settings, לחץ על Control Panel, ולחץ לחיצה כפולה על System.

13. בחר בכרטיסיה User Profile.

שים לב שישנם פרופילי משתמשים רבים המאוחסנים בשרת Server01. פרופילים אלה מייצגים את כל חשבונות המשתמשים שהתחברו לשרת Server01.

14. אל תסגור את יישומון System, כיון שתידרש לו לביצוע ההליך הבא.

הליך 2: הגדרה והקצאה של פרופיל נודד מנדטורי

בהליך זה, תיצור פרופיל נודד מפרופיל משתמש Jane_Doe, ותקצה אותו לחשבון משתמש John Smith. למען הפשטות, בצע את כל השלבים בהליך זה משרת Server01. אם אתה מפעיל את שרת Server02, תוכל גם להתחבר ממחשב זה כדי לבחון את הפרופיל הנודד.

הערה הליך זה יוצא מנקודת הנחה שאתה בקיא ביצירה ושיתוף תיקיה. אם אינך בטוח כיצד לבצע זאת, עיין שוב בפרק 5, תרגיל 1.

---

1. בכונן \:C, צור תיקיה בשם Profiles.

2. שתף את התיקיה C:\Profiles כ- Profiles.

3. פתח את התיקיה Profiles, וצור תת תיקיה בשם Shared. סגור את חלון Profiles.

4. לחץ על לחצן שורת המשימות של תיבת הדו-שיח System Properties. היישומון System אמור להיות פתוח עוד מההליך הקודם.

5. בחר בכרטיסיה User Profiles.

6. תחת Profiles Stored On This Computer, בחר MICROSOFT\Jane_Doe.

7. לחץ על Copy To. תיבת הדו-שיח Copy To תופיע.

8. בתיבת הדו-שיח Copy Profile To, הקלד **\\Server01\profiles\shared**.

9. תחת Permitted To Use, לחץ Change. תופיע תיבת דו-שיח Select User Or Group.

10. בעמודת Name, לחץ Users, ולחץ OK. BUILTIN\Users יופיע באזור Permitted To Use.

11. לחץ OK לחזור לתיבת דו-שיח System Properties. תופיע תיבת הודעות Confirm Copy, המציינת שתיקיה server01\profiles\shared\\ כבר קיימת ושתוכנה הנוכחי יימחק. הודעה זו מופיעה כיון שכבר יצרת את התיקיה עבור הפרופיל.

12. לחץ Yes.

13. לחץ OK לחזור ללוח הבקרה.

14. פתח את תוסף התוכנה Active Directory Users And Computers.

15. הרחב את microsoft.com, ולחץ על התיקיה Users.

16. בחלונית הפרטים, לחץ לחיצה כפולה על חשבון משתמש John Smith. תיבת הדו-שיח John Smith Properties תופיע.

17. בתרגיל קודם, הגדרת את מועד הפקיעה של חשבונו של John Smith. להסרת הגדרה זו, בחר בכרטיסיה Account ובחר Never בחלק של Account Expires.

18. בחר בכרטיסיה Profile.

19. בתיבת נתיב Profile, הקלד **\\server01\profiles\shared**, ולחץ OK. סגור את תוסף התוכנה Active Directory Users And Computers.

    כיון שהנך משתמש בפרופיל מרכזי שניתן להקצות למשתמשים אחרים, השלב הבא הוא להגדיר את הפרופיל כמנדטורי.

20. לחץ לחיצה כפולה My Computer על שולחן העבודה.

21. לחץ לחיצה כפולה על Local Disk (C:).

22. לחץ לחיצה כפולה על Profiles.

23. לחץ לחיצה כפולה על Shared. שים לב שתיקיית User Profile מופיעה.

24. פתח את תפריט Tools, ולחץ על Folder Options. תיבת הדו-שיח Folder Options תופיע.

25. בחר בכרטיסיה View.

26. בחר את לחצן האפשרויות Show Hidden Files And Folders, והסר סימון מתיבת סימון Hide File Extensions For Known File Types.

27. לחץ OK. מופיע חלון Shared, ובו מוצגים קבצים ותיקיות מוסתרות. שים לב שקובץ Ntuser.dat מופיע.

28. בחר בקובץ Ntuser.dat.

29. פתח את תפריט File ולחץ Rename. תיבת שם הקובץ Ntuser.dat מוארת וניתן לערוך אותה.

30. שנה את הסיומת כך ששם הקובץ יהיה Ntuser.man, והקש Enter.

31. סגור את חלון Shared, וסגור את לוח הבקרה.

32. התנתק כמנהל והתחבר שנית כ-John_Smith ללא סיסמה. יופיע שולחן העבודה של John_Smith. שים לב שהמשתמש John_Smith משתמש בערכת צבעים ששייכת לתבנית פרופיל המשתמש, ושקיצור הדרך לדיסק המקומי(:Local Disk (C מופיע בשולחן העבודה.

33. לבדיקת הפרופיל המנדטורי, מחק את קיצור הדרך Connect To The Internet משולחן העבודה.

34. התנתק והתחבר שנית כ- John_Smith ללא סיסמה. שים לב שקיצור הדרך Connect To The Internet שב ומופיע על שולחן העבודה. דבר זה קורה מכיון ששייכת פרופיל מנדטורי לחשבון John_Smith.

הליך 3: הקצאת תיקיית בית למשתמש

בהליך זה, תקצה ל- John_Smith תיקיית בית (Home Folder).

1. התנתק כ- John_Smith והתחבר שנית בשם משתמש Administrator עם הסיסמה password.
2. צור על כונן :C תיקיה בשם HomeDirs.
3. שתף תיקיה זו כ-HomeDirs.
4. פתח את תוסף התוכנה Active Directory Users And Computers.
5. גש למאפייני חשבון משתמש John Smith, ובחר בכרטיסיה Profile.
6. בחלק Home Folder, לחץ על לחצן אפשרויות Connect.
7. ודא ש- :Z מופיע בתיבת הרשימה הנפתחת מימין ל- Connect.
8. בתיבת הטקסט To, הקלד **\\Server01\HomeDirs\%username%**, ולחץ OK.
9. סגור את תוסף התוכנה Active Directory Users And Computers.
10. אתר ולחץ על התיקיה HomeDirs בסייר Windows.
11. פתח את תפריט Files, ולחץ על Properties. תיבת הדו-שיח HomeDirs Properties תופיע.
12. בחר בכרטיסיה Security. שים לב שהקבוצה Everyone מקבלת הרשאת שליטה מלאה בתיקיה זו.
13. לחץ Add. תופיע תיבת דו-שיח Select User, Computers או Groups.
14. בחר Users ולחץ Add.

15. לחץ OK. תיבת הדו-שיח HomeDirs תופיע ובה תצוגה של הקבוצה Everyone Special והקבוצה MICROSOFT\Users. שים לב שלקבוצה Users מוקצות הרשאות Read & Execute (קריאה וביצוע), List Folder Contents (הצג רשימת תכולה של התיקיה) ו-Read (קריאה).

16. הסר סימון מתיבת סימון Allow Inheritable Permissions From Parent To Propagate To This Object. תופיע תיבת הודעות אבטחה.

17. קרא את תיבת הודעות זו, ולחץ Remove. שים לב שלקבוצה Everyone Special אין יותר זכויות בתיקיה HomeDirs.

18. לחץ Add. תופיע תיבת הדו-שיח Select User, Computers, Or Groups.

19. בחר Administrators ולחץ Add.

20. לחץ OK. תיבת הדו-שיח HomeDirs Properties תופיע ובה מוצגות הקבוצה MICROSOFT\Users והקבוצה MICROSOFT\Administrators.

21. ודא שהקבוצה MICROSOFT\Administrators נבחרה.

22. בתיבת ההרשאות (Permissions), לחץ על תיבת סימון Allow בשורת Full Control. כל תיבות הסימון מסומנות.

23. לחץ OK.

24. לחץ לחיצה כפולה על התיקיה HomeDirs.

25. לחץ על John_Smith.

26. פתח את תפריט File ולחץ Properties. תיבת הדו-שיח John_Smith Properties תופיע.

27. בחר בכרטיסיה Security.

שים לב שלמשתמשים בקבוצה Administrators ול-John Smith יש שליטה מלאה בתיקיה זו. הרשאות אלו ניתנו אוטומטית, כאשר הורית לחשבון המשתמש John_Smith להשתמש בתיקיה \\server01\HomeDirs\%username% כתיקיית הבית שלו.

28. לחץ OK, וסגור את סייר Windows.

29. התנתק כמנהל והתחבר שנית כ- John_Smith ללא סיסמה.

30. לחץ לחיצה כפולה על My Computer. שים לב שמופיע סמל של כונן רשת חדש, המצביע על התיקיה John_Smith בשיתוף הרשת \\server01\HomeDirs, והאות המוקצית לו היא :Z.

31. סגור את חלון My Computer, והתנתק.

סיכום שיעור

חשבון משתמש מאפשר למשתמש להתחבר ל-Domain לצורך קבלת גישה למשאבי רשת, או להיכנס למחשב לקבלת גישה למשאבים על מחשב זה. Windows 2000 מספקת חשבונות משתמשים מסוגים שונים: Domain User Accounts ו-Local User Accounts. Windows 2000 מספקת גם Built-In User Accounts, בהם ניתן להשתמש לביצוע מטלות ניהוליות, או לגשת למשאבי רשת. לפני שתתחיל ליצור חשבונות משתמשים, עליך לתכנן מוסכמות למתן שמות לחשבונות אלה, את דרישות הסיסמאות ואפשרויות ההתחברות, כגון שעות התחברות. השתמש בתוסף התוכנה Active Directory Users And Computers ליצירת Domain User Account חדש. השתמש בתוסף התוכנה Local Users And Groups ליצירת Local User Account. לכל חשבון משתמש שנוצר משויכת ערכת מאפייני ברירת מחדל. ניתן לשנות מאפיינים אלה באמצעות תיבת הדו-שיח Properties של כל חשבון משתמש בודד. ניהול חשבונות משתמשים כרוך בשינוי חשבונות משתמשים, בנוסף לניהול פרופילים של משתמשים ותיקיות בית. User Profile (פרופיל משתמש) מכיל אוסף תיקיות ונתונים המגדירים את סביבת שולחן העבודה, הגדרות יישומים של המשתמש, בנוסף לנתונים אישיים. תיקיית בית (Home Folder) היא תיקיה היכולה לשמש לאחסון מסמכים אישיים, ולשמש גם יישומים מיושנים (Legacy Applications). לעיתים היא משמשת כתיקיית ברירת המחדל לשמירת מסמכים.

שיעור 3: ניהול חשבונות קבוצה

שיעור זה מציג בפניך קבוצות, וכיצד הן מיושמות בסביבת Windows 2000. תלמד מהן קבוצות, וכיצד משתמשים בהן לפשט את תהליך ניהול חשבונות משתמשים. פרק זה גם סוקר סוגי קבוצות ומפרט את הכישורים והידע הנדרשים ליישום קבוצות ב-Domain, יישום קבוצות מקומיות וקבוצות מובנות.

לאחר שיעור זה, תוכל

- ליישם קבוצות ב-domain.
- ליישם קבוצות מקומיות וקבוצות מובנות.

זמן לימוד משוער: 60 דקות

מבוא לקבוצות

Group (קבוצה) היא אוסף של חשבונות משתמשים. קבוצות מפשטות ניהול, בכך שהן מאפשרות הקצאת הרשאות וזכויות לקבוצת משתמשים, ולא לחשבונות משתמשים בודדים. משתמשים יכולים להיות חברים ביותר מקבוצה אחת.

בעת הקצאת הרשאות (permissions), אתה נותן למשתמשים את היכולת לגשת למשאבים מסוימים ואתה מגדיר את סוג הגישה שיש להם. לדוגמה, אם מספר משתמשים צריכים לקרוא את אותו קובץ, עליך להוסיף את חשבונות המשתמשים שלהם לקבוצה ולתת לקבוצה הרשאה לקרוא את הקובץ. זכויות (Rights) מאפשרות למשתמשים לבצע מטלות מערכת, כגון שינוי הזמן במחשב, גיבוי או שחזור קבצים, או כניסה מקומית.

בנוסף לחשבונות משתמשים, ניתן להוסיף Contacts, מחשבים וקבוצות אחרות לקבוצה. על ידי הוספת מחשבים לקבוצה, תוכל לפשט את הליך הקצאת מטלת מערכת במחשב אחד, לקבלת גישה למשאבים במחשב אחר.

Groups into a Domain

לפני שתיישם קבוצה ב-Domain, עליך להיות בעל הבנה בסיסית של סוגי קבוצות (Group Types), טווחי קבוצות (Group Scopes), וחברות בקבוצה (Group Membership). מכאן, תוכל ליצור קבוצות, להוסיף חברים לקבוצות, או לשנות את טווח הקבוצה. תוכל אף למחוק קבוצה.

הערה בחלק גדול מתיעוד Windows 2000, Groups into a Domain נקראות פשוט Groups, בעוד שקבוצות אחרות ב-Windows 2000 נקראות Local Groups או Built-In Groups, הנידונות בהמשך שיעור זה. בו בזמן, המושג **Group** (קבוצה) משמש לעיתים קרובות במובן הכללי, ומתייחס לכל סוג קבוצה שניתן ליישם ב-Windows 2000.

סוגי קבוצות

לעיתים תיצור קבוצה מטעמי אבטחה, כגון לשם הקצאת הרשאות. לעיתים תשתמש בקבוצות מטעמים שאינם קשורים לאבטחה, כגון לשליחת דואר אלקטרוני. כדי לסייע בכך, מערכת ההפעלה Windows 2000 Server כוללת שני סוגי קבוצות:

- Security Groups,
- Distribution Groups.

סוג הקבוצה קובע את השימוש בה. שני סוגי הקבוצות כלולים ב-Active Directory Store, המאפשר להשתמש בהם בכל מקום ברשת.

Security Groups

מערכת ההפעלה Windows 2000 משתמשת רק ב-Security Groups (קבוצות אבטחה), המשמשות להקצאת הרשאות גישה למשאבים. תוכנות המיועדות לחפש ב-Active Directory Store יכולות גם הן להשתמש בקבוצות אבטחה מסיבות שאינן קשורות לאבטחה, כגון שליחת הודעות דואר אלקטרוני למספר משתמשים בו-זמנית. מכאן, שלקבוצת אבטחה יש בנוסף את כל היכולות של Distribution Group.

Distribution Groups

יישומים משתמשים ב-Distribution Groups (קבוצות הפצה) כרשימת פעולות שאינן קשורות לאבטחה. השתמש בקבוצות הפצה כאשר הפעילות היחידה של הקבוצה אינה קשורה לאבטחה, כגון שליחת דואר אלקטרוני לקבוצת משתמשים בו-זמנית. לא ניתן להשתמש בקבוצות הפצה להקצאת הרשאות.

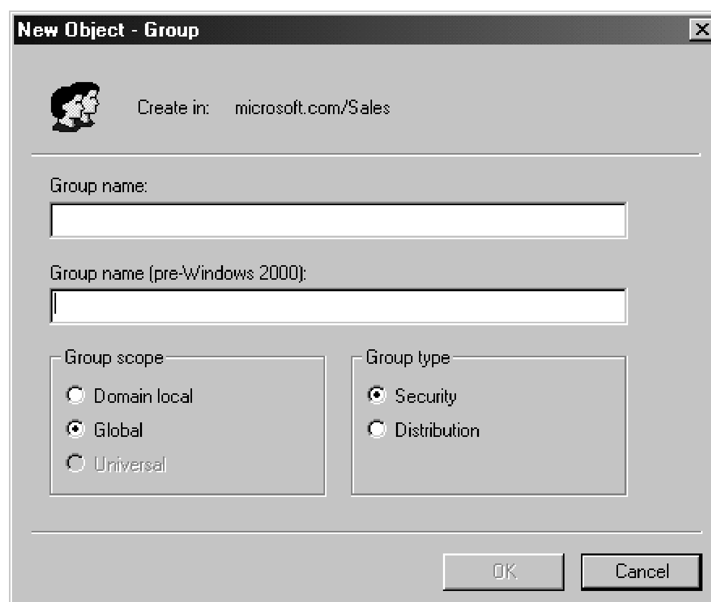
הערה רק תוכנות שנועדו לעבוד עם שירותי Active Directory יכולות להשתמש בקבוצות הפצה. לדוגמה, גרסאות עתידיות של Microsoft Exchange Server יוכלו להשתמש בקבוצות הפצה כרשימות תפוצה לשליחת דואר אלקטרוני.

Group Scopes

בעת יצירת קבוצה, עליך לבחור את סוג הקבוצה (Security או Distribution) ואת Group Scopes (טווח קבוצה) (תרשים 7.8). Group Scopes (טווח הקבוצה) מאפשר שימוש בקבוצה במספר דרכים להקצאת הרשאות.

Group Scopes (טווח קבוצה) קובע היכן ברשת תוכל להשתמש בה. שלושת טווחי הקבוצה הם:

- ❖ Domain Local,
- ❖ Global,
- ❖ Universal.



תרשים 7.8 תיבת הדו-שיח New Object - Group שנפתחה מ- Active Directory Users And Computers ביחידה הארגונית Sales.

Domain Local Groups

Domain Local Groups משמשות לרוב להקצאת הרשאות למשאבים. ל- Domain Local Groups יש את התכונות הבאות:

- ❖ **Open membership** – תוכל להוסיף חברים מכל Domain.
- ❖ **Access to resources in one domain** – ניתן להשתמש ב-Domain Local Group לשם הקצאת הרשאות לגישה רק למשאבים הנמצאים באותו Domain בו יצרת את ה-Domain Local Group.

Global Groups

Global Groups משמשות לרוב לשם ארגון משתמשים להם דרישות גישה דומות לרשת. ל-Global Group יש את התכונות הבאות:

- **Limited membership** – תוכל להוסיף חברים רק מה-Domain בו יצרת את הקבוצה.
- **Access to resources in any domain** – ניתן להשתמש ב-Global Group להקצאת הרשאות לגישה למשאבים הנמצאים בכל domain בעץ או ביער.

Universal Groups

Universal Groups משמשות להקצאת הרשאות למשאבים קשורים ב-Domains רבים. לקבוצת Universal Group יש את התכונות הבאות:

- **Open membership** – תוכל להוסיף חברים מכל Domain.
- **Access to resources in any domain** – ניתן להשתמש ב-Universal Group להקצאת הרשאות גישה למשאבים הנמצאים בכל Domain.
- **Available in Native mode only** – Universal Security Groups אינן זמינות ב-Mixed Mode. ערכת המאפיינים המלאה של Windows 2000 זמינה רק ב-Native Mode. שים לב, בתרשים 7.8, שה-Universal Group אינה זמינה, כיון שהשרת פועל ב-Mixed Mode וסוג הקבוצה מראה שלחצן האפשרויות Security נבחר. ניתן להשתמש ב-Universal Disterbution Group ב-Mixed Mode.

Group Membership

טווח הקבוצה (Group Scope) קובע את החברים בה. חוקי חברות קובעים איזה חברים יכולה קבוצה להכיל. חברים בקבוצה כוללים חשבונות משתמשים וקבוצות נוספות. הטבלה הבאה מתארת חוקי חברות בקבוצה:

טווח קבוצה	**Mixwd Mode**, יכולה להכיל	**Nativ Mode**, יכולה להכיל
Domain Local	חשבונות משתמשים, חשבונות מחשבים, וקבוצות גלובליות מכל Domain	חשבונות משתמשים, חשבונות מחשבים, קבוצות גלובליות, וקבוצות אוניברסליות מכל Domain. בנוסף לקבוצות Domain Local מאותו Domain
Global	חשבונות משתמשים וחשבונות מחשבים מאותו Domain	חשבונות משתמשים, חשבונות מחשבים, וקבוצות גלובליות מאותו Domain
Universal	לא זמין ב- Mixed Mode	חשבונות משתמשים, חשבונות מחשבים, קבוצות גלובליות, וקבוצות אוניברסליות מכל Domain

ניתן להסב Domain Local Groups ו-Global Groups ל-Universal Groups. לביצוע הסבה מוצלחת, נדרש ששירותי Active Directory יהיו ב-Native Mode ושהקבוצות המקומיות, או הקבוצות הגלובליות, לא יכילו חברי קבוצות מאותו טווח קבוצה. לדוגמה, קבוצה Domain Local המכילה קבוצה Domain Local אחרת, לא ניתן להסב אותה לקבוצה אוניברסלית, משום שקבוצה אוניברסלית לא יכולה להכיל קבוצה מסוג Domain Local.

הערה Distibution Groups **הפועלות ב-**Mixed Mode **הן בעלות אותם חוקי חברות כמו** Security Groups **הפועלות ב-**Native Mode**.**

Group Nesting

הוספת קבוצות לקבוצות אחרות (פעולה המכונה קינון קבוצות, Group Nesting) יכולה להפחית את מספר הפעמים שתידרש להקצות הרשאות. עליך ליצור היררכיית קבוצות, המבוססת על הצרכים העסקיים של החברים. Windows 2000 מאפשרת רמות קינון בלתי מוגבלות ב-Native Mode.

לדוגמה, תוכל ליצור קבוצה עבור כל מחלקה בארגון שלך, ואז להוסיף מנהל (manager ולא administrator) מכל מחלקה כדי ליצור קבוצת מנהלי מחלקות. את כל הקבוצות המייצגות את המחלקות הגדר תחת קבוצה אחת גדולה הנקראת WorldWide Managers. כאשר כל המנהלים ברשת נדרשים למשאב כלשהו, הקצה הרשאות לקבוצה WorldWide Managers. כיון שקבוצה זו מכילה את כל חברי קבוצת מנהלי המחלקות באמצעות קינון, כל המנהלים ברשת יכולים לגשת למשאב הנדרש. צורת עבודה זו מאפשרת הקצאה מרוכזת של הרשאות, ובאותה עת מאפשרת הקצאת הרשאות לא ריכוזית על חברות בקבוצה.

בעת הוספת קבוצות לקבוצות אחרות, נסה למזער את רמת הקינון. קינון אמנם מפחית את מספר הפעמים שתקצה הרשאות, אולם, מעקב אחר הרשאות הופך מסובך יותר ככל שעולה מספר רמות הקינון. רמת קינון אחת היא היעילה ביותר, כיון שהיא מפחיתה את מספר הפעמים שנדרש להקצות הרשאות, ומאפשרת מעקב הרשאות קל.

בנוסף, עליך לתעד חברות בקבוצה, כדי לעקוב אחר הקצאת הרשאות. תאר לעצמך תרחיש בו מנהל אחד מוסיף עובדים זמניים לקבוצה שנוצרה עבור עובדים של פרויקט מסוים. בלא שהוא מודע לכך שיש עובדים זמניים בקבוצת הפרויקט, מנהל אחר מוסיף את קבוצת הפרויקט לקבוצה לה יש גישה למידע מסווג של החברה. לעובדים הזמניים יש עתה גישה למידע המסווג של החברה, מצב שאינו קביל.

קינון יעיל של קבוצות בסביבת multiple domain, תפחית את התעבורה בין ה-Domains ברשת ותפשט את ניהול ה-Domain tree. כדי להשתמש בקינון באופן יעיל, עליך להבין את חוקי החברות בקבוצה.

בעת קינון קבוצות, שקול איזה קבוצות ייזמו פחות Cross-Domain Replication. לדוגמה, שכפול (Replication) קבוצות גלובליות נעשה רק על שם הקבוצה ולא על רשימת חבריה, לעומת שכפול קבוצות אוניברסליות המתבצע על שם הקבוצה ורשימת חבריה. בנוסף, עליך לשקול את מצב הפעולה של ה-Domain במסגרת ה-Domain tree:

- ב-Mixed Mode, רק סוג קינון אחד זמין; Universal Groups מכל Domain יכולות להיות חברות של Domain Local Groups. Universal Groups אינן קיימות ב-Mixed Mode.
- ב-Native Mode, כל חוקי החברות בקבוצה זמינים, ומערכת Windows 2000 מאפשרת רמות קינון רבות.

אסטרטגיות קבוצה

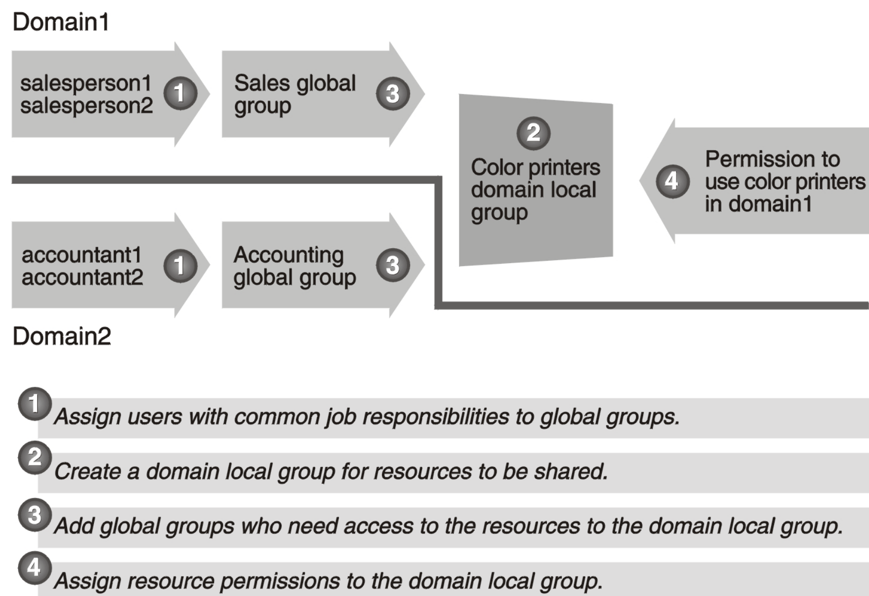
כדי להשתמש בקבוצות ביעילות, עליך לקבוע כיצד תשתמש בקבוצות, ובאיזה סוגי קבוצות תשתמש במצבים מסוימים.

Using Global and Domain Local Groups

הנחיות ליישום Global Groups ו-Domain Local Groups זהות להמלצות אסטרטגיות קבוצות של Windows NT 4.0 או Windows NT 3.x. כאשר אתה מחליט להשתמש ב-Global Groups ו-Domain Local Groups, שקול את ההנחיות הבאות:

- זהה משתמשים בעלי תפקידים דומים, והוסף את חשבון המשתמש שלהם ל-Global Group. לדוגמה, במחלקת הנהלת החשבונות, הוסף את חשבונות המשתמשים של כל מנהלי החשבונות ל-Global Group בשם Accounting.
- זהה איזה משאבים או קבוצת משאבים צריכים המשתמשים, ואז צור Domain Local Group עבור משאב זה. לדוגמה, אם בחברה יש מספר מדפסות צבע, צור Domain Local Group וקרא לה בשם Color Printers.
- זהה את כל ה-Global Groups להן צרכי גישה זהים למשאבים, וצרף אותן כחברות ב-Domain Local Group המתאימה. לדוגמה, הוסף את הקבוצות הגלובליות Accounting, Sales ו-Management ל-Domain Local Group בשם Color Printers.
- הקצה את ההרשאה הנדרשת ל-Domain Local Group. לדוגמה, הקצה את ההרשאות הדרושות לשימוש במדפסות צבע לקבוצה Color Printers.

תרשים 7.9 מתאר את אסטרטגיית השימוש ב-Domain Local Groups: צרף חשבונות משתמשים במסגרת Global Groups, צור Domain Local Groups לקבוצת משאבים שיש לשתפן, צרף את ה-Global Groups ל-Domain Local Group, ואז הקצה הרשאות ל-Domain Local Group. שיטה זו תספק את הגמישות המירבית לגידול ומפחיתה הקצאת הרשאות.



תרשים 7.9 תכנון אסטרטגיית קבוצה.

הערה אסטרטגיית קבוצות מכונה **U, G, DL, P**. הוסף Users לקבוצות Global. הוסף קבוצות Global לקבוצות Domain Local. הקצה Permissions לקבוצות Domain Local.

בנוסף, צירוף חשבונות משתמשים ב-Domain Local Groups והקצאת הרשאות לקבוצה, אינה מאפשרת לך להקצות הרשאות למשאבים מחוץ ל-Domain. אסטרטגיה זו מפחיתה את הגמישות כאשר הרשת שלך גדלה.

למרות היתרון שבשימוש באסטרטגיה זו, צירוף חשבונות משתמשים בקבוצות גלובליות והקצאת הרשאות לקבוצות Domain Local, יכול לסבך את הניהול בעת שימוש ב-Domains רבים. אם יש לאפשר הרשאות דומות לקבוצות גלובליות מ-Domains רבים, עליך להקצות הרשאות לקבוצות אוניברסליות.

Using Universal Groups

Universal Groups (קבוצות אוניברסליות) הן תכונה חדשה של Windows 2000. כאשר אתה מתכנן להשתמש בקבוצות אוניברסליות, שקול את ההנחיות הבאות:

- השתמש בקבוצות אוניברסליות, לתת למשתמשים גישה למשאבים הממוקמים ביותר מ-domain אחד. שלא כמו Domain Local Groups, תוכל להקצות לקבוצות אוניברסליות הרשאות למשאבים בכל domain ברשת. לדוגמה, אם מנהלים (Executive) צריכים לגשת למדפסות ברשת כולה, תוכל ליצור קבוצה אוניברסלית למטרה זו, ולהקצות לה הרשאות שימוש במדפסות על שרתי המדפסות בכל ה-domain.
- השתמש בקבוצות אוניברסליות רק כאשר החברות בהן היא קבועה. ב-Domain Tree, קבוצות אוניברסליות עלולות לגרום לתעבורה מוגברת ברשת בין DCs בכל עת שתשנה את החברות בקבוצה האוניברסלית. זאת, מכיון ששינוי בחברות בקבוצות אוניברסליות עלול להיות משוכפל למספר רב של DCs.
- הוסף קבוצות גלובליות ממספר Domains לקבוצה אוניברסלית, ואז הקצה הרשאות גישה למשאב לקבוצה האוניברסלית. דבר זה מאפשר שימוש בקבוצה אוניברסלית להקצאת הרשאות למשאבים, באופן זהה ל-Domain Local Groups. אולם, שלא כמו ב-Domain Local Group, ניתן להקצות הרשאות לקבוצה אוניברסלית כך שתינתן למשתמשים גישה למשאב הממוקם ב-Domain אחר מזה בו נוצרה הקבוצה.

יישום קבוצות

לאחר שבדקת את צרכי המשתמשים ויש לך תוכנית לקבוצות, אתה מוכן ליישם קבוצות. לפני שתיישם את אסטרטגיה הקבוצות שלך, שקול את ההנחיות הבאות:

- קבע את Group Scope (טווח הקבוצה) הנדרש, בהתאם לשימוש הצפוי בקבוצה. לדוגמה, השתמש ב-Global Groups לקבץ חשבונות משתמשים. השתמש ב-Domain Local Groups או ב-Universal Groups להקצאת הרשאות למשאבים. הקצה Global Groups ל-Domain Local Groups ול-Universal Groups.
- הימנע מהוספת משתמשים בודדים לקבוצות אוניברסליות, כיון שהוספה והסרת משתמשים מקבוצות אוניברסליות תגביר את תעבורת השכפול. לפיכך מומלץ לרכז משתמשים בקבוצות גלובליות ולהוסיף את הקבוצות הגלובליות לקבוצות אוניברסליות.
- ודא שיש לך את ההרשאות הנדרשות ליצירת קבוצה ב-Domain המתאים. כברירת מחדל, לחברים בקבוצה Administrators או בקבוצה Account Operators שב-Domain יש את ההרשאות הנדרשות ליצירת קבוצות. Administrator יכול לתת למשתמש הרשאה ליצירת קבוצות ב-Domain או ב-OU בודדת.

❖ קבע שם לקבוצה. על השם להיות אינטואיטיבי, במיוחד אם administrators מ-Domains אחרים עשויים לחפש אותו בשירותי Active Directory. אם קיימות קבוצות מקבילות במספר Domains, ודא שגם השמות מקבילים. לדוגמה, אם בכל Domain קיימת קבוצת מנהלים (Managers), על קבוצות אלה להיות בעלי שמות במתכונת דומה, כגון Managers USA ו- Managers Israel.

יצירת קבוצות

השתמש בתוסף התוכנה Active Directory Users And Computers ליצירה ומחיקה של קבוצות. בעת יצירת קבוצות, צור אותן ביחידת ארגון User, או ב-OU שיצרת במיוחד עבור קבוצות. ככל שהארגון גדל ומשתנה, אתה עשוי לגלות שיש קבוצות שכבר אין בהן צורך. מחק קבוצות שאינך צריך. כך תוכל לשמור על האבטחה ולא תקצה בטעות הרשאות גישה לקבוצות שאינך זקוק להן יותר.

ליצירת קבוצה, הפעל את תוסף התוכנה Active Directory Users And Computers ובחר ביחידה הארגונית הרצויה. מתפריט Action, הצבע על New ולחץ על Group לפתיחת תיבת הדו-שיח New Object - Group (תרשים 7.8). הטבלה הבאה מפרטת את הנתונים הנדרשים בתיבת הדו-שיח New Object - Group.

אפשרות	תיאור
Group Name	שם הקבוצה החדשה. השם חייב להיות ייחודי ב-domain בו נוצרת הקבוצה.
Group Name (preWindows 2000)	שם הרמה-הנמוכה (תאימות למערכת הפעלה קודמת) של הקבוצה. שדה זה ימולא אוטומטית בהתבסס על שם הקבוצה.
Group Scope	טווח הקבוצה. לחץ Domain Local, Global, או Universal. שים לב שטווח הקבוצה האוניברסלי הוא אפור (לא פעיל) אלא אם נבחרה קבוצה מסוג Distribution, או שהמערכת פועלת ב-Native mode.
Group Type	סוג הקבוצה. לחץ Distribution (הפצה) או Security (אבטחה).

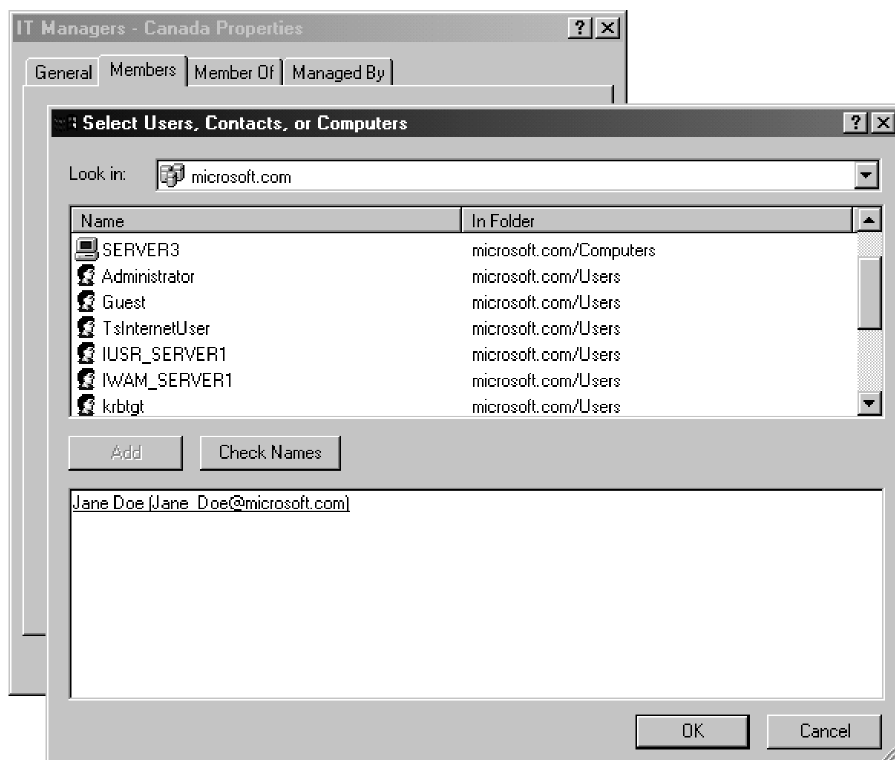
ניהול קבוצות

ניהול קבוצות נעשה באמצעות תוסף התוכנה Active Directory Users And Computers. תוסף תוכנה זה מאפשר ביצוע מספר מטלות ניהוליות, כולל הוספת חברים לקבוצה, שינוי טווח הקבוצה, או מחיקת קבוצה.

הוספת חברים לקבוצה

לאחר שיצרת קבוצה, הוסף לה חברים. חברים בקבוצה יכולים להיות חשבונות משתמשים, אנשי קשר, קבוצות אחרות ומחשבים. ניתן להוסיף מחשב לקבוצה, כדי לאפשר למחשב אחד גישה למשאב משותף במחשב אחר, לדוגמה, לשם גיבוי מרחוק.

להוספת חברים לקבוצה, לחץ לחיצה כפולה על הקבוצה המתאימה. בתיבת הדו-שיח Properties, בחר בכרטיסיה Members ולחץ Add. תופיע תיבת הדו-שיח Select Users, Contacts Or Computers, כמתואר בתרשים 7.10.



תרשים 7.10 תיבת הדו-שיח Select Users, Contacts, Or Computers.

הערה אם ה-Domain שלך ב-Mixed Mode, לא תוכל תמיד להוסיף קבוצות לקבוצה החדשה שלך, תלוי ב-scope של הקבוצה שאתה יוצר.

בתיבת הרשימה הנפתחת Look In, ניתן לבחור Domain ממנו תוכל להציג חשבונות משתמשים, אנשי קשר, מחשבים, וקבוצות. תוכל גם לבחור Entire Directory לעיין בחשבונות משתמשים וקבוצות מכל מקום ב-Active Directory. עתה בחר את חשבון המשתמש או קבוצה שאתה רוצה להוסיף, ולחץ Add.

הערה אם יש צורך להוסיף חשבונות משתמשים רבים או קבוצות, תוכל לחזור ולבצע את הליך בחירתן אחת אחת, ואז ללחוץ Add, או תוכל ללחוץ ולהחזיק את המקשים Shift או Ctrl לבחירת חשבונות משתמשים רבים בבת-אחת. מקש Shift מאפשר בחירת טווח חשבונות רציף, בעוד שמקש Ctrl מאפשר בחירת חשבונות לא רציפים, תוך דילוג. לחץ Add לאחר שבחרת את כל החשבונות שברצונך להוסיף.

לחיצה על Add יוצרת רשימה של החשבונות שבחרת בתיבה Name. לאחר שבחנת את החשבונות, כדאי לוודא שהם החשבונות שאכן ברצונך להוסיף לקבוצה. לחץ OK להוספת החברים.

שינוי טווח הקבוצה (GROUP SCOPE)

עקב שינויים שעשויים להתרחש ברשת, ייתכן שתצטרך לשנות טווח של קבוצה. לדוגמה, ייתכן שתרצה לשנות Domain Local Group קיימת ל-Universal Group, כאשר תצטרך לאפשר למשתמשים לגשת למשאבים ב-domains אחרים. שינוי טווח קבוצה נעשה באמצעות הכרטיסיה General בתיבת הדו-שיח Properties של הקבוצה.

הערה **ניתן לשנות טווח קבוצה רק ב-domain המצוי ב-Native Mode. לא ניתן לשנות טווח** קבוצה ב-Mixed Mode. בנוסף, Windows 2000 אינה מאפשרת שינוי טווח של קבוצות אוניברסליות, כיון שלכל יתר הקבוצות יש חברות וטווח מוגבלים יותר משיש לקבוצה האוניברסלית.

ניתן לבצע את השינויים הבאים לטווח קבוצה:

- **שנה Global Group ל-Universal Group** – תוכל לעשות כן רק אם הקבוצה הגלובלית אינה חברה בקבוצה גלובלית אחרת.
- **שנה Domain Local Group ל-Universal Group** – תוכל לעשות כן רק אם ה-Domain Local Group שאתה מסב אינה מכילה Domain Local Group אחרת.

מחיקת קבוצה

לכל קבוצה שתיצור יש מזהה ייחודי שאינו ניתן לשימוש חוזר, המכונה SID - **S**ecurity **ID**. Windows 2000 משתמשת ב-SID לזיהוי קבוצות והרשאות המוקצות להן. כאשר אתה מוחק קבוצה, Windows 2000 לא תשתמש שוב באותו SID. עקב כך, לא תוכל לשחזר גישה למשאבים על ידי יצירת הקבוצה מחדש, אף אם תיצור קבוצה בעלת שם זהה לקבוצה שמחקת.

בעת מחיקת קבוצה, אתה מוחק רק את הקבוצה ומסיר את ההרשאות והזכויות המשויכות לה בלבד. מחיקת הקבוצה אינה מוחקת את חשבונות המשתמשים החברים בקבוצה. למחיקת קבוצה, לחץ לחיצה ימנית על הקבוצה, ובחר באפשרות Delete.

יישום Local Groups

קבוצה מקומית (Local Group) עשויה להכיל חשבונות משתמשים במחשב, וניתן להקצותה למשאבים במחשב זה. השתמש בקבוצות מקומיות להקצאת הרשאות למשאבים השוכנים על המחשב המקומי בו נוצרה הקבוצה המקומית. Windows 2000 יוצרת קבוצות מקומיות במסד נתוני האבטחה המקומיים. ישנם שני סוגים של קבוצות מקומיות:

- Domain,
- Non-Domain.

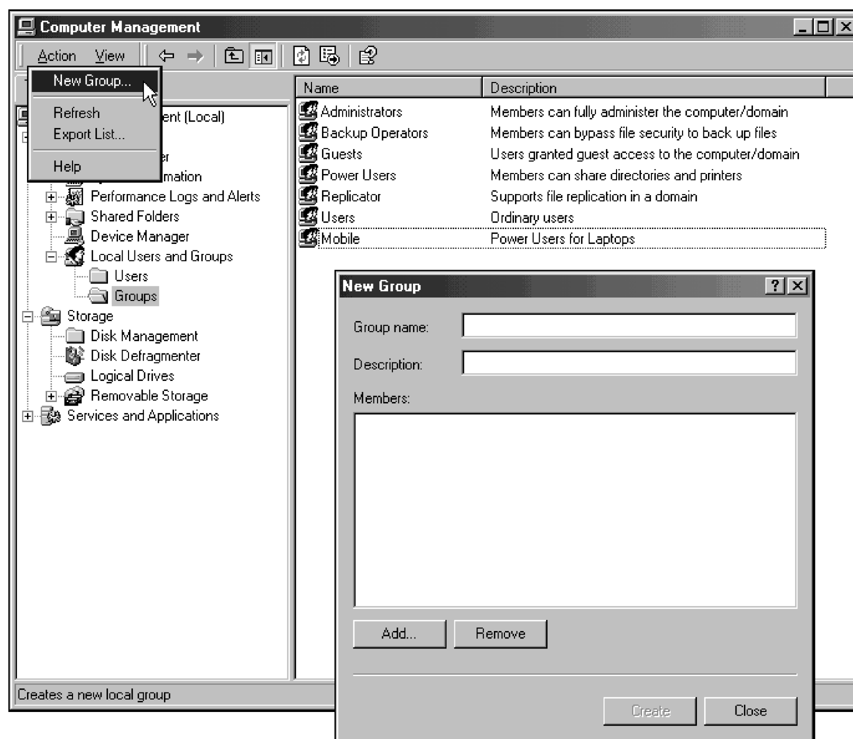
להלן מספר הנחיות לשימוש בקבוצות מקומיות:

- Domain Local Groups נוצרות ב-Active Directory Store ומשמשות את כל ה-DCs שב-Domain. ניתן להקצות קבוצה מקומית ל-domain לכל משאב הפועל על ה-DCs שב-domain.
- Non-domain Local Groups נוצרות בשרתים עצמאיים, שרתים-חברים, ובמחשבים הפועלים תחת Windows 2000 Professional. אולם, ניתן להשתמש בקבוצות מקומיות אלה רק במחשב בו נוצרה הקבוצה המקומית. לכן, אין להשתמש ב-Non-domain Local Groups במחשבים שהם חלק מ-Domain. שימוש ב-Non-domain Local Groups מונע ריכוז ניהול הקבוצות. Non-domain Local Groups לא מופיעות ב-Active Directory Store. יש לנהלן בנפרד עבור כל מחשב.
- תוכל להקצות הרשאות Non-domain Local Groups לגישה רק למשאבים במחשב בו יצרת את הקבוצות המקומיות.

Non-domain Local Groups מכילות חשבונות משתמשים עבור המחשב בו יצרת את הקבוצה המקומית. בנוסף, קבוצות אלה אינן יכולות להיות חברות בקבוצה אחרת.

יצירת Local Groups

השתמש בתוסף התוכנה Computer Management ליצירת Non-domain Local Groups. אתה יוצר קבוצות מקומיות בתיקיה Groups (תרשים 7.11). ליצירת קבוצה מקומית, הרחב את Local Users And Groups בחלון Tree ובחר Groups. מתפריט Action, לחץ New Group. הכנס שם ותיאור עבור הקבוצה.



תרשים 7.11 יצירת Local Group חדשה במערכת Windows 2000 Professional.

הטבלה הבאה מתארת את האפשרויות המוצגות בתיבת הדו-שיח New Group:

אפשרות	תיאור
Group Name	שם ייחודי לקבוצה המקומית. זה הנתון היחיד שנדרש. השתמש בתו כלשהו פרט ללכסון הפוך (backslash) (\). השם יכול להכיל עד 256 תווים; אולם, לא ניתן להציג שמות ארוכים מאד בחלון אחד.
Description	תיאור הקבוצה.
Add	הוסף משתמש לרשימת החברים.
Remove	הסר משתמש מרשימת החברים.
Create	צור קבוצה

ניתן להוסיף חברים לקבוצה מקומית בעת יצירתה או לאחר יצירתה.

הערה Windows 2000 Server ששודרג ל-DC יציג את תוסף התוכנה Local Users and Groups עם סימן איקס (X) אדום ולא יאפשר גישה אליו, משום שמחשב הפועל כ- Windows 2000 DC לא מאפשר יצירת חשבונות מקומיים.

Built-In Groups

למערכת Windows 2000 יש ארבע קטגוריות של קבוצות מובנות: Global, Domain Local, Local, System.

ל-Built-In Groups יש ערכה קבועה-מראש של זכויות משתמשים או חברות בקבוצה. Windows 2000 יוצרת קבוצות אלה עבורך, כך שלא תצטרך ליצור קבוצות ולהקצות זכויות והרשאות לתפקידים נפוצים.

הערה קבוצות מובנות אינן ניתנות למחיקה.

Built-In Global Groups

Windows 2000 יוצרת Built-In Global Groups כדי לקבץ סוגים נפוצים של חשבונות משתמשים. כברירת מחדל, Windows 2000 מוסיפה חברים באופן אוטומטי לכמה Built-In Global Groups. תוכל להוסיף חשבונות משתמשים ל-Built-In Groups אלה ולספק זכויות והרשאות למשתמשים נוספים, בזמן שאתה מקצה אותן ל-built-in group.

בעת יצירת domain, Windows 2000 יוצרת Built-In Global Groups ב-Active Directory. אתה מקצה הרשאות או על ידי הוספת Global Groups ל-Domain Local Groups, או הקצאת הרשאה מפורשת ל-Built-In user groups.

יחידת הארגון User מכילה את ה-Built-In Global Groups שב-Domain. הטבלה מתארת את חברות ברירת המחדל של ה-Built-In Global Groups השכיחות ביותר.

קבוצה גלובלית	תיאור
Domain Users	כל חשבון משתמש חדש ב-Domain הופך אוטומטית לחבר בקבוצה זו. חשבון Administrator חבר בקבוצה זו כברירת מחדל.
Domain Admins	חשבון Administrator חבר בקבוצה זו כברירת מחדל. כדי שחברים בקבוצת Domain Admins ב-Domain אחד יוכלו לבצע מטלות ניהוליות ב-Domain אחר, יש להוסיף את קבוצת Domain Admins לקבוצת Administrator המקומית של ה-Domain האחר.
Domain Guests	חשבון Guest חבר בקבוצה זו כברירת מחדל. (חשבון Guest אינו פעיל (Disable) כברירת מחדל).
Enterprise Admins	הקבוצה הגלובלית הזו נוצרת רק ב-Root Domain המשמש כשורש ב-Forest. כברירת מחדל חברים בקבוצה זו חשבון Administrator וקבוצת Administrators מקומית של Root Domain. לחברים בקבוצה זו יש שליטה מלאה בכל ה-Domains מבלי שיהיה צורך להוסיפם לקבוצת Domain Users ב-Domains האחרים. כאשר משנים Mixed Mode למצב Native ב-Domain, משתנה טווח הקבוצה מטווח גלובלי לטווח אוניברסלי.

הערה כדי להציג חברים בקבוצה (מכל סוג), פתח את כרטיסיית Members מתוך מאפייני (Properties) הקבוצה או את כרטיסיית Members of כדי לצפות בקבוצות אליהן קבוצה נוכחית זו שייכת.

Built-In Domain Local Groups

Windows 2000 יוצרת Built-in Domain Local Groups ב-Domain כדי לספק למשתמשים זכויות והרשאות לביצוע מטלות על DCs וב- Active Directory. Built-In Domain Local Groups פועלת באופן זהה לזה בו פועלת Domain Local Group. ההבדל היחיד הוא ש-Built-In Domain Local Group לא ניתנת למחיקה.

Built-In Domain Local Groups מספקות זכויות מוגדרות מראש והרשאות לחשבונות משתמשים בעת הוספת חשבונות משתמשים או Global Groups כחברים. הטבלה הבאה מתארת את ה-Built-In Domain Local Groups השכיחות ביותר, ואת היכולות של החברים בהן.

קבוצות Domain Local	תיאור
Account Operators	חברים בקבוצה זו יכולים ליצור, למחוק, ולשנות חשבונות משתמשים וקבוצות; הם אינם יכולים לבצע שינויים בקבוצה Administrators או באיזה מבין הקבוצות Operators.
Server Operators	חברים בקבוצה זו יכולים לשתף משאבי דיסק, לגבות ולשחזר קבצים על DC.
Print Operators	חברים בקבוצה זו יכולים להגדיר ולנהל מדפסות רשת ב-DC.
Administrators	חברים בקבוצה זו יכולים לבצע את כל מטלות הניהול בכל ה-DCs וב- domain. כברירת מחדל, בחשבון זה חברים חשבון Administrator, הקבוצה הגלובלית Domain Admins והקבוצה הגלובלית/אוניברסלית Enterprise Admins.
Guests	חברים בקבוצה זו יכולים לבצע רק מטלות שהקצת להן זכויות ולגשת רק למשאבים להם הקצית הרשאות; חברים בקבוצה זו אינם יכולים לבצע שינויים קבועים לסביבת שולחן העבודה שלהם. כברירת מחדל, חשבון משתמש Guest והקבוצה הגלובלית Domain Guests חברים בקבוצה זו. שירותים מסוימים מוסיפים משתמשים באופן אוטומטי לקבוצה זו בעת התקנתם. לדוגמה, Internet Information Services - IIS מוסיף חשבונות משתמשים אנונימיים לקבוצה Guest המובנית.
Backup Operators	חברים בקבוצה זו יכולים לגבות ולשחזר את כל ה-DCs באמצעות Windows Backup.

קבוצה גלובלית	תיאור
Users	חברים בקבוצה זו יכולים לבצע רק מטלות שהקצת להם זכויות ולגשת רק למשאבים שלהם הקצית הרשאות. כברירת מחדל, הקבוצה Domain Users, הקבוצה המיוחדת Authenticated Users והקבוצה המיוחדת INTERACTIVE, הם חברים בקבוצה זו. קבוצות המערכת מתוחזקות על ידי Windows 2000 ולא ניתן להסירן מהמערכת. השתמש ב-User Built-In Local Group להקצאת הרשאות וזכויות שצריכות להיות לכל משתמש עם חשבון משתמש ב-Domain שלך.

Built-In Local Groups

לכל ה-Stand-Alone Servers (שרתים עצמאיים), Member servers (שרתים-חברים), ומחשבים המפעילים Windows 2000 Professional, יש Built-In Local Groups הנותנות זכויות לביצוע מטלות על מחשב בודד, כגון גיבוי ושחזור קבצים, שינוי זמן במערכת, וניהול משאבי המערכת. Windows 2000 שומרת את Built-In Local Groups בתיקיה Groups של תוסף התוכנה Computer Management. כמו Domain Built-In Groups, לא ניתן למחוק Built-In non-domain local groups.

הטבלה שלהלן מתארת את היכולות של חברים ב-Built-In Local Groups השכיחות ביותר.

קבוצה מקומית	תיאור
Users	חברים בקבוצה זו יכולים לבצע רק מטלות עבורן נתת זכויות ולגשת רק למשאבים שלהם הקצית הרשאות. כברירת מחדל, Windows 2000 מוסיפה חשבונות משתמשים מקומיים שיצרת על מחשב זה לקבוצה Users. כאשר שרת חבר או מחשב הפועל תחת Windows 2000 Professional מתחבר ל-domain, Windows 2000 מוסיפה את הקבוצה הגלובלית Domain Users Global Group, את הקבוצה המיוחדת Authenticated Users, ואת הקבוצה המיוחדת INTERACTIVE לקבוצה המקומית Users.
Administrators	חברים בקבוצה זו יכולים לבצע את כל מטלות הניהול במחשב. כברירת מחדל, חשבון המשתמש המובנה Administrator עבור המחשב הוא חבר בקבוצה זו. בעת ששרת חבר על מחשב המפעיל Windows 2000 Professional מצטרף ל-domain, Windows 2000 מוסיפה את הקבוצה Domain Admins לקבוצה Administrators המקומית.

קבוצה מקומית	תיאור
Guests	חברים בקבוצה זו יכולים לבצע רק מטלות שהקצת להם זכויות ולגשת רק למשאבים שלהם הקצית הרשאות; הם אינם יכולים לבצע שינויים קבועים לסביבת שולחן העבודה שלהם. כברירת מחדל, חשבון Guest המובנה של המחשב הוא חבר בקבוצה זו. חשבון זה אינו פעיל בעת ההתקנה. כאשר שרת חבר או מחשב המפעיל Windows 2000 Professional מצטרף ל-Domain, לא מתוספות קבוצות מה-Domain לקבוצה זו.
Backup Operators	חברים בקבוצה זו יכולים להשתמש ב- Windows Backup לגיבוי ושחזור המחשב.
Power Users	חברים בקבוצה זו יכולים ליצור ולשנות חשבונות משתמשים מקומיים על המחשב, ולשתף משאבים.
Replicator	חברים בקבוצה זו יכולים להגדיר שירותי שכפול קבצים.

Built-In Special Identities Groups

Special Identities Groups, הידועות כקבוצות מערכת ב-Windows NT, קיימות בכל מחשב המפעיל Windows 2000. לקבוצות Special אין חברות מסוימת שניתן לשנות, אך הן יכולות לייצג משתמשים שונים בזמנים שונים, תלוי כיצד משתמש ניגש למחשב או משאב. אינך רואה קבוצות Special כאשר אתה מנהל קבוצות, אך הן זמינות לשימוש כאשר אתה מקצה זכויות והרשאות למשאבים. Windows 2000 מבססת חברות בקבוצת Special על אופן הגישה למחשב, לא על מי משתמש במחשב. הטבלה הבאה מתארת את Special Identities Groups השכיחות ביותר.

קבוצה מיוחדת	תיאור
Everyone	כולל את כל המשתמשים הניגשים למחשב. היזהר אם אתה מקצה הרשאות לקבוצת Everyone ומאפשר את החשבון Guest. Windows 2000 תואמת משתמש שאין לו חשבון משתמש תקף כאורח. המשתמש יקבל אוטומטית את כל הזכויות וההרשאות שהקצת לקבוצת Everyone.
Authenticated Users	כולל את כל המשתמשים עם חשבון משתמש תקף במחשב או בשירותי Active Directory. השתמש בקבוצת Authenticated Users במקום קבוצת Everyone, כדי למנוע גישה אנונימית למשאבים.

קבוצה מיוחדת	תיאור
Creator Owner	כולל את חשבון המשתמש של משתמש שיצר או לקח בעלות על משאב. אם חבר בקבוצה Administrators יוצר משאב, קבוצה זו היא בעלת המשאב.
Network	כולל כל משתמש שיש לו קישור ממחשב אחר ברשת למשאב משותף במחשב.
Interactive	כולל את חשבון המשתמש עבור המשתמש המחובר למחשב. חברים בקבוצה האינטראקטיבית יכולים לגשת למשאבים על המחשב אליו הם מחוברים פיסית. הם מתחברים ומקבלים גישה למשאבים על ידי "שיתוף פעולה" עם המחשב.
Anonymous Logon	כולל כל חשבון משתמש ש-Windows 2000 לא אימתה.
Dialup	כולל כל משתמש שיש לו חיבור נוכחי שנעשה באמצעות חיוג.

תרגיל 4: שינוי מצב ה-domain

בתרגיל זה, תשתמש בתוסף התוכנה Active Directory Users And Computers לשינוי מצב ה-Domain.

הליך 1: שינוי מ-Mixed Mode ל-Native Mode

ברירת המחדל של מצב העבודה של Windows 2000 Server הוא Mixed Mode. כדי לנצל את כל התכונות המתייחסות לקבוצות ב-Windows 2000 Server, על ה-Domain שלך להיות ב-Native Mode. בצע את התרגיל להלן בשרת Server01.

1. היכנס לשרת Server01 בשם משתמש Administrator עם הסיסמה password.
2. פתח את תוסף התוכנה Active Directory Users And Computers.
3. בחלון Tree, בחר ב-domain שלך, פתח את תפריט Action, ולחץ על Properties. תופיע תיבת דו-שיח microsoft.com Properties. שים לב שה-Domain שלך כרגע ב-Mixed Mode. כמו כן, שים לב לאזהרה בדבר שינוי מצב ה-Domain.
4. לחץ Change Mode. תיבת ההודעות של Active Directory תופיע ותזהיר ששינוי זה בלתי הפיך. לחץ Yes. תיבת הדו-שיח microsoft.com Properties תראה ששינית את מצב ה-domain ל-Native mode.

5. לחץ OK לסגור את תיבת הדו-שיח microsoft.com Properties. תופיע תיבת הודעות של Active Directory המעידה שהפעולה הושלמה בהצלחה ושייקח 15 דקות או יותר עד שמידע זה ישוכפל בכל ה-DCs.
6. לחץ OK.
7. שמור את תוסף התוכנה Active Directory Users And Computers פתוח, כיון שתשתמש בו בתרגיל הבא.

תרגיל 5: יצירת קבוצות

בתרגיל זה, תיצור קבוצת אבטחה גלובלית. לאחר מכן תוסיף לקבוצה זו חברים. להוספת חברים לקבוצה, תוסיף שתי חשבונות משתמשים, Jane Doe ו- John Smith שיצרת בעבר. לאחר מכן תיצור Domain Local Group, בה תשתמש להקצאת הרשאות גישה לדוחות מכירות (Sales Reports). לבסוף, תאפשר גישה לדוחות המכירות לחברי קבוצת האבטחה הגלובלית, על ידי הוספת קבוצת האבטחה הגלובלית ל-Domain Local Group. בצע תרגיל זה על שרת Server01.

הליך 1: יצירת קבוצה גלובלית, הוספת חברים וארגון חשבונות משתמשים

בהליך זה, תיצור קבוצת אבטחה גלובלית, תוסיף חברים לקבוצה, ואז תעביר משתמש מיחידה ארגונית אחת לשנייה.

1. ודא שתוסף התוכנה Active Directory Users And Computers פתוח ושהוא נמצא בקידמה.
2. בחלון Tree, לחץ על היחידה הארגונית Sales.

   בחלונית הפרטים, יופיע חשבון משתמש Jane Doe.
3. פתח את תפריט Action, הצבע על New, ולחץ Group. תופיע תיבת הדו-שיח New Object - Group (אובייקט חדש - קבוצה).

   שים לב שכאשר נבחרת קבוצה מסוג Security, טווח קבוצה אוניברסלית זמין. הוא זמין עקב כך ששירותי Active Directory פועלים כעת במצב Native.
4. ודא שלחצן אפשרויות Global מסומן, ושלחצן אפשרויות Security מסומן אף הוא.
5. הקלד **Sales** בתיבת הטקסט Group Name, ולחץ OK. הקבוצה תופיע בחלון הפרטים של היחידה הארגונית Sales.
6. בחלונית הפרטים, לחץ לחיצה כפולה על Sales. תיבת הדו-שיח Properties של Sales תציג את מאפייני הקבוצה.

7. בחר בכרטיסיה Members.

8. לחץ Add. תופיע תיבת הדו-שיח Select Users, Computers, Or Groups, והרשימה הנפתחת Look In תראה microsoft.com.

9. ברשימה, בחר Jane_Doe, לחץ והחזק את מקש Ctrl, ולחץ על John_Smith.

שני חשבונות המשתמשים נבחרו. שים לב ש- Jane Doe היא ביחידה הארגונית microsoft.com/Sales ו-John Smith נמצא ביחידה הארגונית microsoft.com/Users.

10. לחץ Add. Jane Doe ו-John Smith הם עתה חברים בקבוצה הגלובלית Sales Security.

11. לחץ OK.

12. לחץ OK שנית לסגירת תיבת הדו-שיח Sales Properties. מסיבות ארגוניות, החלטת להעביר את John Smith ליחידה הארגונית Sales.

13. לחץ על היחידה הארגונית Users.

14. לחץ על חשבון משתמש John Smith בחלונית הפרטים.

15. לחץ Action ולחץ Move. חלון Move יופיע.

16. לחץ על היחידה הארגונית Sales בחלון Move, ולחץ OK. חשבון משתמש John Smith נעלם מחלונית הפרטים של היחידה הארגונית Users.

17. בחלון Tree, לחץ על היחידה הארגונית Users. John Smith, Jane Doe וקבוצת האבטחה הגלובלית Sales יופיעו בחלונית הפרטים.

18. לחץ לחיצה כפולה על הקבוצה הגלובלית Sales. תיבת הדו-שיח Sales Properties תופיע.

19. לחץ Members. שים לב שחשבון משתמש John Smith נשאר חבר בקבוצה, אך התיקיה Active Directory מוגדרת עכשיו microsoft.com/Sales.

20. לחץ OK.

21. הישאר ביחידה הארגונית Sales, והמשך להליך הבא.

הליך 2: יצירה ושימוש ב-Domain Local Group

בהליך זה, תיצור Domain Local Group שתשמש להקצאת הרשאות גישה לדוחות מכירות. כיון שהקבוצה משמשת להקצאת הרשאות, הפוך אותה ל-Domain Local Group. לאחר מכן תוסיף חברים לקבוצה, על ידי הוספת קבוצת האבטחה הגלובלית שיצרת בהליך 1.

1. לחץ על חלונית הפרטים, כדי שקבוצת המכירות הגלובלית אינה נבחרת יותר.
2. פתח את תפריט Action, הצבע על New, ולחץ Group. תופיע תיבת הדו-שיח New Object - Group.
3. בתיבת הטקסט Group Name, הקלד Reports.
4. עבור סוג הקבוצה, ודא שנבחר Security, ועבור Group Scope, לחץ על Domain Local.
5. לחץ OK. ה-Domain Local Group תופיע בחלונית הפרטים של היחידה הארגונית Sales.
6. בחלונית הפרטים של היחידה הארגונית Sales, לחץ לחיצה כפולה על Reports.

   תיבת הדו-שיח Reports Properties תציג את תכונות הקבוצה.
7. בחר בכרטיסיה Members.
8. לחץ Add. תופיע תיבת הדו-שיח Select Users, Contacts, Computers Or Groups.
9. לחץ על החץ כלפי מטה שבתיבת הרשימה הנפתחת Look In, ובחר Entire Directory.

   יופיעו כל חשבונות המשתמשים והקבוצות מכל Domain או אתר של כל חשבון משתמש או קבוצה.
10. מעל רשימת חשבונות המשתמשים, קבוצות ומחשבים, לחץ על העמודה Name. העמודה Name ממוינת לפי סדר אלפא-ביתי, בסדר יורד.
11. לחץ על העמודה Name פעם נוספת, כדי למיין אותה בסדר עולה.
12. לחץ Sales, לחץ Add, ולחץ OK. קבוצת Sales היא עתה חברה ב-Reports domain local group.
13. לחץ OK.
14. סגור את תוסף התוכנה Active Directory Users And Computers.

הליך 3: יישום אבטחת NTFS

בפרק 4, למדת על הרשאות NTFS. בהליך זה, תקצה הרשאות NTFS לקבוצה המקומית שיצרת בהליך הקודם, ואז תבחן את הגישה לתיקיה Sales. בצע תרגיל זה משרת Server01.

1. צור בכונן :C תיקיה בשם Dept.
2. שתף את התיקיה Dept כ-Dept, ובתיבת הטקסט Comment, הקלד **Department Share**.

   אין צורך להגדיר הרשאות על השיתוף כיון שהתיקיה Dept נוצרה על NTFS volume**.**
3. צור תת תיקיה תחת תיקיית Dept, ותן לה שם **Sales.**
4. לחץ על התיקיה Sales.
5. פתח את תפריט File ולחץ Properties. תיבת הדו-שיח Sales Properties תופיע.
6. בחר בכרטיסיה Security. שים לב שלקבוצת המיוחדת Everyone ניתנת שליטה מלאה על תיקיה זו.
7. הסר סימון מתיבת סימון Allow Inheritable Permissions From Parent To Propagate To This Object. תיבת ההודעה Security תופיע ותודיע לך מה האפשרויות.
8. לחץ Remove. תופיע תיבת הדו-שיח Sales Properties.
9. לחץ Add. תופיע תיבת הדו-שיח Select Users, Contacts, Computers Or Groups.
10. בחר Entire Directory בתיבת הרשימה הנפתחת Look In.
11. בחר את Reports domain local group, ולחץ Add.
12. לחץ OK. בתיבת הדו-שיח Sales Properties, לקבוצה המקומית Reports, מוקצות הרשאות Read & Execute (קריאה וביצוע), List Folder Contents (הצגת תכולת התיקיה), ו-Read (קריאה).
13. סמן את תיבת הסימון Write, ולחץ OK.
14. סגור את חלון Dept, והתנתק כמנהל.
15. התחבר כ- Jane_Doe עם הסיסמה student, וגש לתיקיה C:\Dept\Sales ב-My Computer.
16. לחץ על תפריט File, הצבע על New, ולחץ על Text Document. הקובץ New Text Document יופיע בחלון Sales.
17. לחץ לחיצה כפולה על New Text Document. פנקס הרשימות (Notepad) יופיע ובו הקובץ החדש פתוח.

18. הקלד מספר אותיות, וסגור את פנקס הרשימות. תופיע תיבת הודעות השואלת אם ברצונך לשמור את השינויים.

19. לחץ Yes.

20. סגור את חלון Sales.

21. התנתק כ- Jane_Doe והתחבר כ- Bob_Train ללא סיסמה. אם אינך מצליח להתחבר כ-Bob Train, בדוק לראות אם אתה מתחבר בזמן שהגדרת ש- Bob Train אינו יכול להתחבר. הגדרת זאת בתרגיל קודם בפרק זה.

22. נסה לגשת לתיקיה C:\Dept\Sales. תופיע תיבת הודעות Dept המודיעה שהגישה נמנעה.

הגישה לחשבון משתמש Bob Train נמנעה, כיון שאינו חבר בקבוצה הגלובלית Sales אשר הפכה חברה ב-domain local group, Reports. שים לב, שגם גישה מקומית אינה מתאפשרת. זאת כיון שהרשאות NTFS מגבילות את הגישה הרשתית והמקומית גם יחד.

23. לחץ OK וסגור את חלון Dept.

24. התנתק כ- Bob Train.

סיכום שיעור

קבוצה (Group) היא אוסף חשבונות משתמשים, אנשי קשר, מחשבים וקבוצות אחרות. ישנם שני סוגים של קבוצות ב-Windows 2000: Security ו-Distribution. מערכת ההפעלה Windows 2000 משתמשת רק ב-Security Groups, המשמשות להקצאת הרשאות גישה למשאבים. יישומים משתמשים ב-Distribution Groups כרשימות לפעולות לא מאובטחות. בנוסף להגדרתן לפי סוג, קבוצה מוגדרת גם על ידי טווח. קיימים שלושה טווחי קבוצות: Domain Local, Global, Universal. Domain Security Groups משמשות בדרך כלל להקצאת הרשאות למשאבים, ואילו Global Groups משמשות בדרך כלל לארגן משתמשים להם דרישות דומות לגבי גישה לרשת. Universal Groups משמשות לרוב להקצאת הרשאות למשאבים קרובים ב-Domains רבים. טווח הקבוצה קובע את החברות בקבוצה. חוקי חברות כוללים את החברים שקבוצה יכולה להכיל והקבוצות בהן קבוצה יכולה להיות חברה. כאשר אתה מוכן ליצור את הקבוצה שלך ב-Domain, השתמש בתוסף התוכנה Active Directory Users And Computers. תוסף תוכנה זה מאפשר גם ניהול קבוצות, הכולל הוספת חברים לקבוצה, שינוי טווח הקבוצה, ומחיקת קבוצה. ליצירת Non-domain Local Group, השתמש בתוסף התוכנה Computer Management.

שיעור 4: Group Policies

Group Policy (מדיניות קבוצה) מספקת מנגנון נוסף לחידוד, עידון וריכוז הניהול של סביבת שולחן העבודה של המשתמש. מדיניות קבוצה יכולה לשמש לשליטה על התוכנות הזמינות למשתמש, התוכנות המופיעות על שולחן העבודה של המשתמש, ואפשרויות תפריט ההתחלה (Start).

מדינויות קבוצה מוגדרות עבור אתרים (Sites), Domain ויחידות ארגון (OUs) ומשמשות לאכיפת מדיניות חברה. מדינויות קבוצה משפיעות על חשבונות משתמשים, קבוצות, מחשבים ו-OUs שאתה מנהל. עליך לדעת ולהכיר את מדינויות הקבוצה השונות.

לאחר שיעור זה, תוכל

- להסביר את מבנה מדיניות הקבוצה, כולל אובייקטים של מדיניות קבוצה, מכולות ותבניות.
- להסביר את ההיררכיה של יישום מדיניות קבוצה, כולל חוק הירושה ושיטות לשינוי הורשת מדיניות.
- להשתמש בתוסף התוכנה Active Directory Users And Computers ליצירת אובייקט מדיניות קבוצה ולשנות את ההגדרות באובייקט זה.
- להשתמש בתוסף התוכנה Group Policy להגדרת מדיניות קבוצה למשתמשים ומחשבים.

זמן לימוד משוער: 90 דקות

מבוא למדיניות קבוצה

מדיניות קבוצה היא אוסף הגדרות תצורה המיושם על אובייקט אחד או יותר ב-Active Directory. מנהל Group Policy משתמש במדיניות קבוצה לבקרה על סביבות העבודה של משתמשים ב-Domain. מדיניות קבוצה יכולה גם לבקר את סביבת העבודה של משתמשים עם חשבונות הממוקמים ב-OU מסוימת. בנוסף, ניתן להגדיר מדיניות קבוצה ברמת Site, תוך שימוש בתוסף התוכנה Active Directory Sites And Services.

Group Policy מורכבת מהגדרות המכתיבות התנהגות אובייקט ב-Active directory. מדיניות קבוצה מאפשרת ל-Group Policy Administrator לספק למשתמשים סביבת שולחן עבודה מאוכלסת בכל האמצעים הדרושים. סביבה זו יכולה לכלול תפריט התחלה אישי, יישומים המוגדרים אוטומטית, והגבלות גישה לקבצים, תיקיות והגדרות מערכת של Windows 2000. Group Policy (מדיניות קבוצה) יכולה גם להשפיע על זכויות הניתנות לחשבונות משתמשים וקבוצות.

ייתכנו התנגשויות בין מדיניות קבוצה וצרכים מקומיים, כגון כאשר מדיניות מגבילה את יכולתו של משתמש לגשת למשאב הנדרש לו לביצוע עבודתו. כאשר זה קורה, עליך לעבוד עם Group Policy Administrator כדי לפתור את הבעיה. לדוגמה, אם מדיניות קבוצה המיושמת ברמת ה-domain מונעת ממשתמשים ברשת לגשת ליישום הנדרש להם לביצוע עבודתם, התקשר ל-Group Policy Administrator לתקן את המצב.

יש חריג לצורך להתקשר תמיד ל-Group Policy Administrator; על ידי שחרור חשבון משתמש מנעילה שנוצרה על ידי מדיניות הקבוצה.

יתרונות של מדיניות קבוצה

Total **C**ost Of **O**wnership (TCO), העלות הכוללת של הבעלות) היא העלות הכרוכה בניהול רשתות מבוזרות של מחשבים אישיים. מחקרים אחרונים בנושא TCO מראים שחוסר יעילות של המשתמשים היא אחת העלויות הגדולות של חברות. חוסר היעילות הוא לא אחת תוצאה של שגיאת משתמש, כגון שינוי קבצי תצורת מערכת ובכך הפיכת המחשב לבלתי שמיש, או שהיא מיוחסת לריבוי תכונות ויישומים שאינן חיוניות והמבלבלות את המשתמש.

ניתן להפחית את ה-TCO של הרשת שלך, על ידי החלת Group Policy ליצירת סביבת שולחן עבודה ה"תפורה" לתפקיד ורמת המיומנות של המשתמש.

אבטחה של סביבת עבודה של משתמש

כמנהל רשת בעלת רמת אבטחה גבוהה, אתה עשוי לרצות ליצור סביבת עבודה נעולה במחשב. על ידי יישום מדיניות קבוצה נדרשת למשתמשים מסוימים, בשילוב עם הרשאות NTFS, פרופילים מנדטוריים, ותכונות אבטחה נוספות של Windows 2000, תוכל למנוע ממשתמשים להתקין תוכנות ולגשת לתוכנות ונתונים לא מאושרים. כמו כן תוכל למנוע ממשתמשים למחוק קבצים החשובים לתפקוד נכון של היישומים ומערכות ההפעלה שלהם.

שיפור סביבת העבודה של המשתמש

תוכל להיעזר במדיניות קבוצה לשפר את סביבת העבודה של המשתמש כדלקמן:

- העברה אוטומטית של יישומים לתפריט ההתחלה של המשתמש.
- אפשר הפצת יישומים, כך שמשתמשים יוכלו לאתר יישומים ברשת בקלות ולהתקינם.
- העברת קבצים או קיצורי דרך למקומות שמישים ברשת או לתיקיה מסוימת במחשב של משתמש.
- בניית מערך אוטומטי של מטלות או תוכנות קבועות בעת התחברות או ניתוק משתמש לרשת, כאשר המחשב מתחיל לפעול או מכובה.
- ניתוב תיקיות למקומות ברשת להגברת אמינות וזמינות הנתונים.

הערה למידע נוסף אודות מדיניות קבוצה, עיין בתקליטור המצורף לספר זה (\chapt07\articles\Outline For Group Policy Design Readiness White Paper 3.doc ו- \chapt07\articles\GroupPolicyWhitePaperBeta3.doc).

סוגי מדיניות קבוצה

מדיניות קבוצה משפיעה על מיגוון רכיבי רשת ואובייקטים של Active Directory. הטבלה להלן מתארת את סוגי מדיניות הקבוצה:

סוג מדיניות קבוצה	תיאור
Software Settings	משפיע על היישומים שמשתמש יכול לגשת אליהם. מדיניות זו יוצרת התקנת יישומים אוטומטית בשתי דרכים: • Assigned - מדיניות הקבוצה מתקינה או משדרגת יישומים אוטומטית על מחשבי הלקוחות או מספקת למשתמש חיבור ליישום, אשר הוא אינו יכול למחוק. • Published - מנהל מדיניות הקבוצה מפרסם תוכנות באמצעות שירותי Active Directory. אז מופיעים היישומים ברשימת הרכיבים הפעילים שמשתמש יכול להתקין על ידי שימוש ביישומון לוח הבקרה Add/Remove Programs. משתמשים יכולים לבטל התקנת יישומים אלה.
Scripts	מאפשרים למנהלי מדיניות קבוצה להגדיר תסריטים וקבצי אצווה כך שיפעלו בזמנים מסוימים, כגון בעת הפעלת או כיבוי המערכת, או כאשר משתמש מתחבר או מתנתק. תסריטים יוצרים מערך אוטומטי של מטלות חוזרות על עצמן, כגון מיפוי כונני רשת.
Security Settings	מאפשרים למנהלי מדיניות קבוצה להגביל גישת משתמשים לקבצים ותיקיות, להגדיר הגבלת חשבונות (כגון כמה פעמים יכול משתמש להקליד סיסמה שגויה לפני שהמערכת נועלת את חשבון המשתמש שלו), להגדיר מדיניות מקומית (כגון זכויות משתמש וביקורת), לבקר פעולת השירות, להגביל גישה לרישום ויומן אירועים, להגדיר גישת מפתח ציבורי, ולהגדיר מדיניות אבטחת IP (IPSec).
Administrative Templates	כולל מדיניות קבוצה מבוססת-רישום המערכת (Registry Based Policy), המשמשת להגדרת מאפייני רישום (Registry)שיכתיבו את התנהגות ומראה שולחן העבודה, כולל רכיבי מערכת ההפעלה ויישומים.

סוג מדיניות קבוצה	תיאור
RIS- **R**emote **I**nstallation **S**ervices	שולטים על אפשרויות התקנת RIS המוצגות למשתמש בעת הרצת אשף התקנת לקוח RIS.
Folder Redirection	מאפשר הפניית תיקיות Windows 2000 מיוחדות ממיקום ברירת המחדל של הפרופיל שלהן למיקום חליפי ברשת, בו ניתן לנהלן בצורה מרכזית.

Group Policy Structure

Group Policies (מדיניות קבוצה) הן אוסף הגדרות תצורה הניתן להחיל על אובייקט אחד או יותר ב-Active Directory. הגדרות אלה נמצאות בתוך **G**roup **P**olicy **O**bject (**GPO**, אובייקט מדיניות קבוצה). GPO מאחסנים מידע על מדיניות קבוצה בשני מקומות : מכולות (Containers) ותבניות (Templates).

GPO - Group Policy Objects

GPO - **G**roup **P**olicy **O**bjects מכיל הגדרות Group Policy עבור sites, domains, ו-OUs. GPO מכילים תכונות הנכתבות ל-Active Directory באובייקט המכונה GPC (**G**roup **P**olicy **C**ontainer, מכולת מדיניות קבוצה). בנוסף, GPO מאחסנים נתוני מדיניות קבוצה במבנה תיקיה המכונה GPT (**G**roup **P**olicy **T**emplate, תבנית מדיניות קבוצה). מבנה התשתית של GPO נסתר בעיקרו מה-administrator.

ניתן ליישם GPO אחד או יותר ל-Site, doamin או OU. מכולות רבות ב-Active Directory יכולות להשתייך לאותו GPO, ומכולה בודדת יכולה להשתייך ליותר מ-GPO אחד. סינון טווח ה-GPO מבוצע על ידי חברות בקבוצות אבטחה.

נתוני מדיניות קבוצה בעלות מימדים קטנים והמשתנים לעיתים רחוקות, מאוחסנים ב-GPC. מדיניות קבוצה בעלת מימדים גדולים והעשויה להשתנות לעיתים תכופות, מאוחסנת ב-GPT.

Local Group Policy Objects

Local GPO קיים בכל מחשב Windows 2000, וכברירת מחדל, רק תצורת האבטחה מוגדרת. ה-Local GPO מאוחסן בתיקיה %systemroot%\System32\GroupPolicy, ויש לו את הרשאות ACL הבאות:

- **Administrators** (מנהלים) – שליטה מלאה.
- **SYSTEM** (מערכת) – שליטה מלאה.
- **Authenticated Users** (משתמשים מורשים) – קריאה וביצוע, הצגת רשימת תכולתה של התיקיה וקריאה.

הערה SYSTEM **ו-** Authenticated Users **הן** built-in special Groups.

Group Policy Containers

GPC - **G**roup **P**olicy **C**ontainers הוא אובייקט Active Directory המאחסן תכונות GPO ומכיל תת-מכולה לנתוני מחשב ומידע על מדיניות קבוצות משתמשים. GPC מכיל מידע על הגירסה הנוכחית, כדי לוודא שהמידע המאוחסן ב-GPC מתואם עם המידע ב-GPT. GPC כולל גם נתוני מצב סטטוס המעידים האם GPO פעיל או לא.

GPC מאחסן את נתוני Windows 2000 Class Store להחלת יישומים. **Class Store**, הוא מחסן מבוסס-שרת לכל היישומים, ממשקים ו-API המספקים את יכולות פרסום (Published) והקצאה (Assigned).

Group Policy Templates

GPT הוא מבנה תיקיה השוכן בתיקיה של ה-DCs בשם %systemroot%\SYSVOL\sysvol\<**domain_name**\Policies. GPT היא המכולה בה הגדרות מדיניות לתבניות ניהוליות, הגדרות אבטחה, קבצי תסריט, והגדרות תוכנה מאוחסנות.

מבנה GPT

בעת יצירת GPO, נוצר גם מבנה תיקיית GPT המתאים. שם התיקיה שניתן ל-GPT הוא ה-GUID של ה-GPO שנוצר. לדוגמה, אם נוצר GPO המשויך ל-domain בשם microsoft.com, תיקיית GPT שתיווצר תיקרא כדלקמן:

%systemroot%\SYSVOL\sysvol\microsoft.com\Policies\
{45265FA6-554F-4F74-97CC-61B4663DAE61}

הערה ה-GUID שניתן לעיל - דוגמה בלבד.

תכולת GPT

בדרך כלל, תכולת ברירת המחדל של GPT היא תת התיקיות Users, Machine וקובץ Gpt.ini. בעודך יוצר ומשנה מדיניות, נוצרות תיקיות נוספות. מבנה התיקיות המסוים תלוי במדיניות הקבוצה שהגדרת. הטבלה הבאה מתארת כמה תת-תיקיות המצויות בדרך כלל במבנה GPT:

תת תיקיה	תכולה
\Adm	קבצי תבנית adm. המשויכים לקבצי GPT הם קבצי טקסט המעובדים על ידי Windows 2000 להחיל שינויים על רישום המערכת (Registry).
\User	קובץ Registry.pol עם הגדרות רישום להחלה על משתמשים.
\User\Applications	קבצי הפרסום (קבצי aas.) המשמשים את Microsoft Windows Installer.
\User\Documents & Settings	קובץ כלשהו להפצה לשולחן העבודה של המשתמש כחלק מ-GPT זה.
\User\Scripts	תיקיות ההתחברות והניתוק
\Users\Scripts\Logon	תסריטים וקבצים שמתייחסים לתסריטים של Logon Scripts.
\Users\Scripts\Logoff	תסריטים וקבצים שמתייחסים לתסריטים של Logoff Scripts.
\Machine	קובץ Registry.pol המכיל את הגדרות הרישום אותן יש להחיל על המחשב.
\Machine\Applications	קבצי הפרסום (קבצי aas) המשמשים את Microsoft Windows Installer.
\Machine\Documents & Settings	כל קובץ המיועד להפצה לכל שולחנות העבודה של כל המשתמשים המתחברים למחשב זה כחלק מ-GPT זה.
\Machine\Microsoft\WindowsNT\SecEdit	קובץ GptTmpl.ini של עורך האבטחה (Security Editor).
\Machine\Scripts	תת תיקיות ההפעלה והכיבוי.
\Machine\Scripts\Startup	התסריטים וקבצים המתייחסים ל-Startup Scripts.
\Machine\Scripts\Shutdown	התסריטים וקבצים המתייחסים ל-Shutdown Scripts.

קובץ Gpt.ini

תיקית השורש של כל GPT מכילה קובץ בשם Gpt.ini. ניתן להכניס את הנתונים הבאים לקובץ זה:

- **Version=x** – כאשר x הוא מספר גרסת GPO. מספר הגירסה מתחיל ב- 0 בעת יצירת ה-GPO לראשונה, וגדל על ידי הוספת 1 באופן אוטומטי בכל עדכון של ה-GPO.
- **Disabled=y** – כאשר y הוא או 1 או 0 ומתייחס רק ל-GPO המקומי. מתג זה מציין אם ה-GPO המקומי מאופשר או מבוטל. קובץ Gpt.ini מגדיר אם ה-GPO המקומי מאופשר (Enable) או מבוטל (Disable); עבור כל שאר ה-GPO, מידע זה מאוחסן ב-GPC שבמחסן Active Directory.

קובץ Registry.pol

קובץ Registry.pol שבתת התיקיה User מורד ומוחל (applied) על החלק HKEY_CURRENT_USER של רישום המערכת (Registry) כאשר המשתמש מתחבר. קובץ Registry.pol בתת התיקיה Machine מורד ומוחל על חלק HKEY_LOCAL_MACHINE של הרישום בהליך האתחול של המחשב.

פורמט קבצי Registry.pol שונה מזה הנוצר תוך שימוש בעורך System Policy של Windows 95, Windows 98, או Windows NT 4.0. קבצים הנוצרים על ידי שימוש בגירסה קודמת של System Policy Editor לא ניתנים להחלה על מחשבי Windows 2000, וקבצים שנוצרו באמצעות תוסף התוכנה Group Policy של Windows 2000 לא ניתן להחיל על מחשבים הפועלים תחת מערכות הפעלה Windows 95, Windows 98 או Windows NT 4.0.

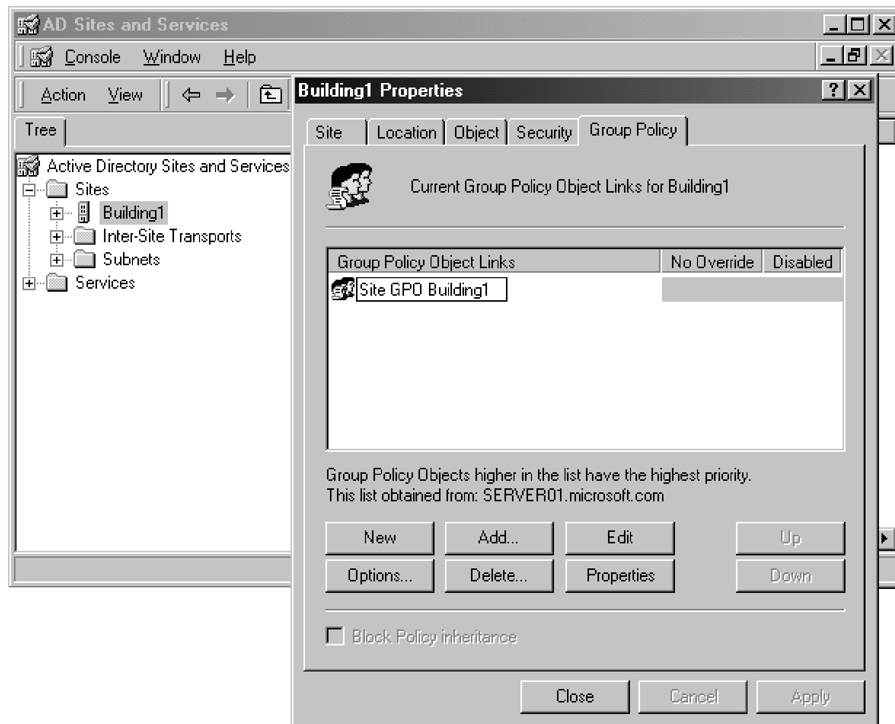
יישום Group Policies

לפני שתוכל ליצור מדיניות קבוצה, עליך ליצור אובייקטים שיכילו מדיניות קבוצה. משם תוכל לערוך מדיניות קבוצה, לנהל הרשאות ולנהל ירושה (Inheritance).

יצירת GPO

השלב הראשון ביצירת Group Policy (מדיניות קבוצה) הוא ליצור או לפתוח GPO. ניתן ליצור אובייקט מדיניות קבוצה, ל-Domain או OU, באמצעות תוסף התוכנה Active Directory Users And Computers. ניתן ליצור אובייקט מדיניות קבוצה ל-Site על ידי שימוש בתוסף התוכנה Active Directory Sites And Services. בשני המקרים, ההליך זהה.

ליצירת אובייקט מדיניות קבוצה, פתח את ה-Properties עבור Site, ה-Domain או אובייקט ה-OU. בתיבת הדו-שיח Properties, בחר בכרטיסיה Group Policy. לחץ New והקלד שם עבור האובייקט. תרשים 7.12 מתאר כיצד ליצור GPO.



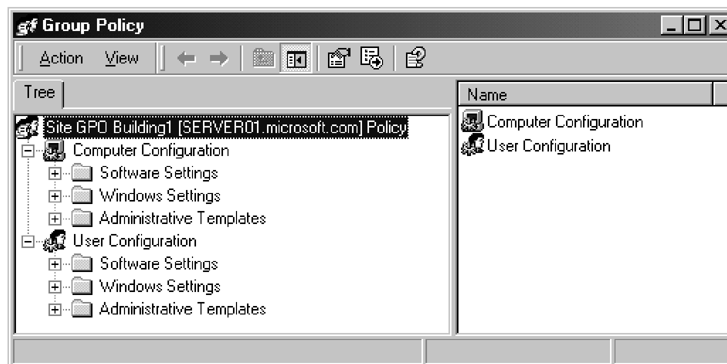
תרשים 7.12 יצירת אובייקט מדיניות קבוצה עבור Site בשם Building1.

הערה תוכל גם להוסיף GPO קיים על ידי לחיצה על Add ובחירת GPO מ-Sites, Domains או OUs.

שימוש בתוסף התוכנה Group Policy

תוסף התוכנה Group Policy הוא הכלי העיקרי של ה-Administrator להגדרה ובקרה, כיצד ינהגו תוכנות, משאבי רשת, ומערכת ההפעלה עבור משתמשים ומחשבים בארגון. בסביבת שירותי Active Directory, מדיניות קבוצות מוחלת על משתמשים או מחשבים על בסיס חברות ב-Sites, Domains או OUs.

לאחר שיצרת GPO, תוכל להשתמש בתוסף התוכנה Group Policy להגדרת מדיניות קבוצה למחשבים וחשבונות משתמשים. תרשים 7.13 מתאר את תוסף התוכנה Group Policy.



תרשים 7.13 תוסף התוכנה Group Policy המופיע בעת לחיצת לחצן Edit, כמתואר בתרשים 7.12.

ממשק תוסף התוכנה Group Policy

ממשק תוסף התוכנה Group Policy כולל את Computer Configuration ואת User Configuration. כל אחד מהם מציג את ההרחבות הבאות:

- ❖ Software Settings - הגדרת תוכנה.
- ❖ Windows Settings - הגדרת Windows.
- ❖ Administrative Templates - תבניות ניהול.

תצורת המחשב

תיקיות Computer Configuration מכילות הגדרות, המסייעות בהגדרת סביבת עבודה אישית עבור המשתמש, או אכיפת מדיניות נעילה עבור מחשבים ברשת. מדינויות תצורת מחשב מיושמות בעת אתחול המערכת. אם תקצה מדיניות משתמשים למחשבים, מדיניות המשתמשים חלה על כל משתמש המתחבר למחשב, ללא תלות ב-OU אליה שייך המשתמש.

תצורת משתמש

תיקיות User Configuration מכילות הגדרות, המסייעות בהגדרת סביבת עבודה אישית עבור המשתמש, או אכיפת מדיניות נעילה עבור משתמשים ברשת. הגדרות אלה כוללות את כל המדינויות ייחודיות-המשתמש, כגון מראה שולחן העבודה, הגדרת יישומים, תסריטי התחברות וניתוק, ויישומים מוקצים וציבוריים. מדינויות User Configuration מיושמות בעת התחברות למחשב.

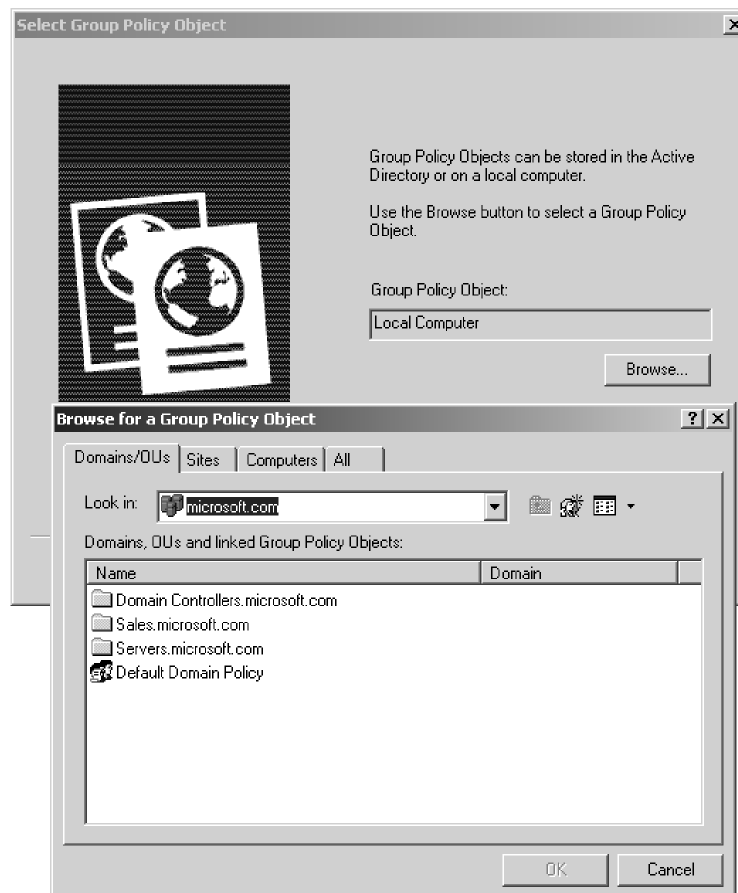
שימוש בתוסף התוכנה Group Policy

כל מופע של תוסף התוכנה Group Policy, הוא ייחודי ל-GPO מסוים. תוכל להוסיף תוסף תוכנה Group Policy ייחודי-GPO ל-MMC Console, כך שישמש ככלי עצמאי. דבר זה מאפשר לך להוסיף תוסף תוכנה לכל GPO שתרצה לנהל. כמו כן, תוכל לפתוח את

תוסף התוכנה Group Policy עבור GPO מסוים דרך Site, Domain או OU בו הוא ממוקם. לבסוף, תוכל לערוך את ה-Local GPO באמצעות Gpedit.msc.

יצירת MMC Console

על ידי שימוש ב-MMC Console, תוכל ליצור כלי הכולל תוסף תוכנה Group Policy עבור כל GPO שברצונך לנהל. לאחר פתיחת ממשק MMC, הוסף Group Policy כתוסף תוכנה עצמאי. כאשר אתה מוסיף את תוסף התוכנה, עליך לבחור את ה-GPO המשויך לתוסף התוכנה. תוכל להוסיף את ה-Local GPO, שהוא ברירת המחדל, או שתוכל לעיין ולאתר GPO הנמצאים ב-Sites, Domains או OUs (תרשים 7.14). כמו כן תוכל לעיין ולאתר את ה-GPO המקומי במחשב כלשהו ב-domain שלך. לאחר שהוספת את תוסף התוכנה Group Policy עבור כל GPO שבכוונתך לנהל, שמור את MMC Console כקובץ MSC. עתה תוכל לפתוח את הקובץ בכל עת, כדי לנהל את ה-GPO שהוספת לעמדה. כמו כן, תוכל להוסיף או למחוק GPO כנדרש.



תרשים 7.14 עיון לאיתור כל ה-Group Policy שנוצרו ב-Domain בשם microsoft.com.

עריכת GPO ב-Sites, Domains ו-OUs

ליצירה ועריכה של GPO, פתח את תוסף התוכנה Group Policy עבור GPO מסוים מ-site, domain או OU. עבור Sites, השתמש בתוסף התוכנה Active Directory Sites And Services. עבור Domains ו-OUs, השתמש בתוסף התוכנה Active Directory Users And Computers. פתח את תיבת הדו-שיח Properties עבור ה-Site, Domain, או OU, ובחר בכרטיסיה Group Policy. בחר את ה-GPO שברצונך לנהל, ולחץ Edit. פעולה זו תטען את תוסף התוכנה Group Policy עבור אובייקט מסוים זה. מהלך ניווט זה מתואר בתרשימים 7.12 ו- 7.13. בשלב זה, תוכל לערוך את ה-GPO כנדרש.

שימוש בקובץ Gpedit.msc

תוכל לערוך את ה-GPO המקומי באמצעות קובץ Gpedit.msc. בתיבת הטקסט Open של הפקודה Run, הקלד **Gpedit.msc**, ולחץ OK. פעולה זו תטען את תוסף התוכנה Group Policy עבור ה-GPO במחשב המקומי. מכאן, תוכל לערוך את ה-GPO כנדרש.

תוכל לבצע ניהול מדיניות מרחוק על ידי שימוש בפרמטר gpcomputer:**<computername>** או בפרמטר gpobject יחד עם Gpedit.msc. המשתנה **computername**, בשימוש עם gpcomputer, יכול להיות שם NetBios או שם DNS. לצפייה ולהגדרה ב-GPO של ה-domain עבור Server01 ב-domain ששמו microsoft.com, תוכל להקליד:

```
gpedit.msc /gpcomputer:"server01"
```

או

```
gpedit.msc /gpcomputer:"server01.microsoft.com"
```

הפרמטר gpcomputer מתוכנן להציג את ה-GPO של ה-domain. הפרמטר gpobject מחייב נתיב ADSI ויכול לפתוח כל GPO שנוצר במחסן Active Directory. לדוגמה, לפתוח GPO עם GUID של 45265FA6-554F-4F74-97CC-61B663DAE61 ב-domain בשם microsoft.com, תוכל להקליד:

```
gpedit.msc/gpobject:"LDAP://CN={45265FA6-554F-4F74-97CC-
61B4663DAE61} ,CN=Policies, CN=System, DC=microsoft, DC=com"
```

הרשאות GPO

כאשר אתה יוצר GPO (אובייקט מדיניות קבוצה), ערכת קבוצות מתוספת לאובייקט, וכל קבוצה כזו מוגדרת עם מספר מאפיינים. ברירת המחדל היא הקצאת הרשאות ל-GPO מסוג Read, Write, Create All Child Objects, Delete All Child Objects. לקבוצה המיוחדת Creator Owner מוקצות גם הרשאות מיוחדות לניהול אובייקטים צאצאים בתוך ה-GPO. לקבוצה המיוחדת Authenticated Users ניתנת הרשאת מדיניות קבוצה מסוג Read And Apply. שים לב, שכברירת מחדל, מאפיין Apply Group Policy מוענק רק לקבוצה Authenticated Users. פרט לקבוצה Authenticated Users, חברים בקבוצות אחרות יכולים לערוך את ה-GPO. הגדרות המדיניות הכלולות ב-GPO אינן ישימות לחברים בקבוצה שנמנעה ממנה ההרשאה Apply Group Policy.

Administrators יכולים להגדיר לאיזה קבוצת מחשבים ומשתמשים תהיה ההרשאה Apply Group Policy לאובייקט. קבוצות שיש להן ההרשאה Apply Group Policy וההרשאה Read ל-GPO מקבלות את מדיניות הקבוצה המוגדרת הכלולה באובייקט.

הטבלה הבאה היא רשימה של קבוצות ברירת המחדל של GPO ותכונותיהן :

קבוצת אבטחה	הגדרות ברירת המחדל
Authenticated Users	Read, **A**pply **G**roup **P**olicy (AGP)
Creator Owner	הרשאות אובייקט ומאפיין מיוחדות המוקצות לאובייקטים צאצאים ותכונות בתוך ה-GPO.
Domain Admins	Read ,Write ,Create All Child Objects Delete All Child Objects
Enterprise Admins	Read ,Write ,Create All Child Objects Delete All Child Objects
System	Read ,Write ,Create All Child Objects Delete All Child Objects

גם Administrators הם משתמשים מורשים, והמשמעות היא שיש להם את ערכת המאפיינים Apply Group Policy. אם זה אינו נדרש, ל-Administrators יש שתי אפשרויות:

- ❖ הסרת משתמשים מורשים מהרשימה, והוספת קבוצת אבטחה אחרת, כאשר המאפיין Apply Group Policy מוגדר Allow. קבוצה זו צריכה להכיל את כל המשתמשים שה-GPO אמור להשפיע עליהם.
- ❖ הגדר מאפיין Apply Group Policy כ-Deny עבור קבוצות Domain Admins ו- Enterprise Admins, ואולי אף לקבוצת Creator Owner. בכך תמנע יישום GPO על חברים בקבוצות אלו. זכור שלהרשאת Deny תמיד תהיה עדיפות על הרשאת Allow. אי לכך, אף אם חבר שייך לקבוצה אחרת לה הרשאת Apply Group Policy, עדיין לא תיושם עליו מדיניות זו.

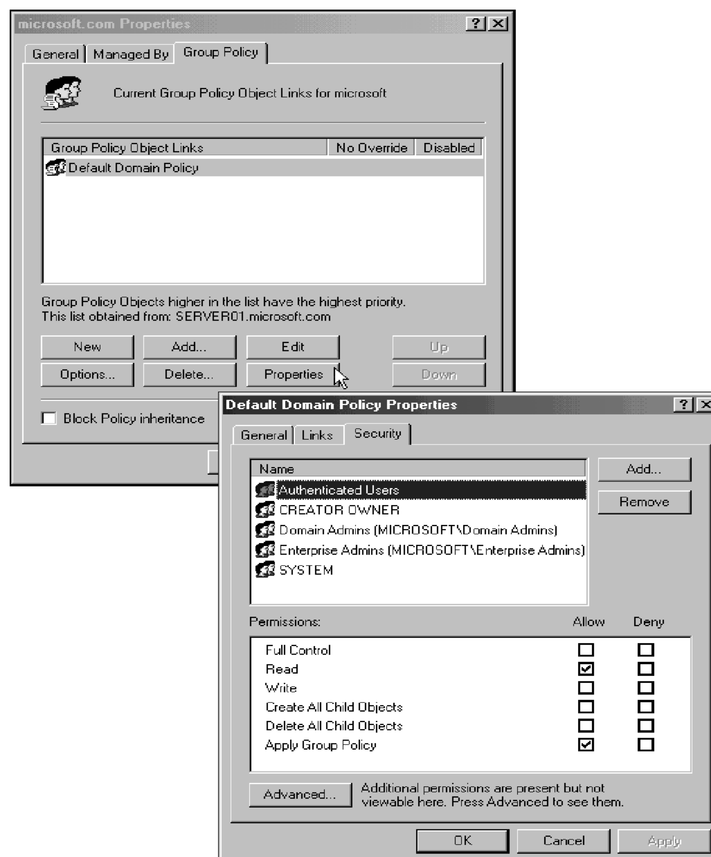
לעריכת GPO, על המשתמש להיות בעל הרשאת כתיבה וקריאה לאובייקט. לא ניתן לפתוח GPO במצב קריאה-בלבד. במילים אחרות, אם ניתן לפתוח את תוסף התוכנה Group Policy, אז ניתן לערוך את אובייקט Group Policy המופיע ב-Namespace. יתרה מזאת, השינויים חלים בעת העריכה: אין שלב Save או Activate. Administrator עשוי לרצות לנתק את הקשר בין GPO ל-Site, Domain או OU בעת העריכה, או שירצה לשמור על הקשר אך לבטל (Disable) את צמתי המחשב והמשתמש.

לא ניתן להשתמש בקבוצות אבטחה להחלת (או הסרת) רק חלק מההגדרות שבאובייקט Group Policy - פרט למקרים של ניתוב תיקיות והתקנת תוכנה, להן יש ACL נוספים המוגדרים ברמת ה-GPO, כדי לשפר עוד יותר את ההתנהגות בהתבסס על חברות בקבוצת אבטחה.

לעריכת GPO, על המשתמש להיות אחד מהבאים:

- ❖ Administrator
- ❖ Creator Owner
- ❖ משתמש שניתנה לו גישה לאובייקט Group Policy.

ניתן לשנות הרשאות של GPO על ידי פתיחת תיבת הדו-שיח Properties עבור ה-Site, Domain או OU המכילה את ה-GPO ואז בחירה בכרטיסיה Group Policy. בחר את ה-GPO, לחץ Properties, ובחר בכרטיסיה Security, כמתואר בתרשים 7.15.



תרשים 7.15 גישה להגדרות האבטחה של microsoft.com Defualt Domain Policy GPO..

משם, תוכל לשנות את ההרשאות הבסיסיות או ללחוץ על Advanced לשינוי הרשאות מתקדמות.

סדר ההורשה (Inheritance)

ככלל, הגדרות מדיניות קבוצה מועברות בירושה ממכולת הורה (Parent container) למכולת הצאצא (Child container). אם הקצת מדיניות קבוצה מסוימת למכולת הורה ברמה גבוהה, מדיניות הקבוצה חלה על כל המכולות שמתחת למכולת ההורה, כולל אובייקטים של משתמשים ומחשבים בכל מכולה. אולם, אם תגדיר מדיניות קבוצה באופן מפורש עבור מכולת צאצא, הגדרות מדיניות סותרות של הקבוצה במכולת הצאצא דורסות את הגדרות מכולת ההורה.

אם ל-OU של ההורה יש הגדרות מדיניות שלא הוגדרו, צאצא ה-OU אינו יורש אותן. מדיניות קבוצה שבוטלו (Disabled) עוברות בירושה כמבוטלות. כמו כן, אם מדיניות הוגדרה ל-OU של הורה, ומדיניות זהה לא הוגדרה ל-OU של הצאצא, הצאצא יירש את הגדרת המדיניות של ההורה.

אם מדיניות הורה וצאצא תואמות, הצאצא יירש את מדיניות ההורה, וגם הגדרות הצאצא מיושמות. מדיניות עוברת בירושה כל עוד הן תואמות. לדוגמה, אם מדיניות הורה גורמת לכך שתיקיה מסוימת תופיע על שולחן העבודה, ומדיניות הצאצא קוראת לתיקיה נוספת, המשתמש יראה את שתי התיקיות.

אם מדיניות המוגדרת ל-OU של הורה אינה תואמת עם מדיניות זהה המוגדרת ל-OU של צאצא, הצאצא לא יירש את הגדרת המדיניות מההורה. ההגדרה של הצאצא היא זו שתהיה מיושמת.

תוכל להשתמש בתוסף התוכנה Active Directory Users And Computers להגדרת ירושות עבור domains ו-OUs. פתח את תיבת הדו-שיח Properties של ה-Domain או ה-OU, ובחר בכרטיסיה Group Policy. בנוסף, תוכל להגדיר ירושות ל-Domains על ידי שימוש בתוסף התוכנה Active Directory Sites And Services. פתח את תיבת הדו-שיח Properties עבור ה-Site המסוים, ובחר בכרטיסיה Group Policy. יש שתי אפשרויות להגדרת ירושה:

- תיבת הסימון Block Policy Inheritance,
- תיבת הסימון No Override.

Block Policy Inheritance

תוכל לחסום ירושת מדיניות ברמת ה-domain או ה-OU על ידי שימוש בתיבת הסימון Block Policy Inheritance. תיבת סימון זו ממוקמת בכרטיסיה הראשונה של תיבת הדו-שיח Properties של כל GPO. חסימת מדיניות ירושה אינה זמינה למדיניות site, כיון שאתר נמצא בראש היררכית GPO. אם אפשרות זו נבחרת עבור אובייקט מדיניות קבוצה ברמת-צאצא, הצאצא אינו יורש מדיניות כלשהי מאובייקט מדיניות קבוצה ברמת-הורה.

No Override

תיבת הסימון No Override מאלצת את כל מכולות מדיניות צאצא לרשת את מדיניות ההורה, אף אם מדיניות זו סותרת את מדיניות הצאצא, ואף אם חסימת מדיניות ירושה (Block Inheritance) הוגדרה עבור הצאצא. תיבת סימון No Override והתיבה הבאה המתוארת נגישות על ידי לחיצה על Options, בתיבת הדו-שיח Properties של ה-GPO.

Disabled

תיבת הסימון Disabled מכבה את ה-GPO כך שאינו פעיל יותר. אולם, הוא עדיין משויך למכולה בה הוא הוגדר. ככלל, אפשרות זו משמשת לשינוי הגדרות במדיניות בלי להשפיע על המשתמשים. לאחר שהשינויים הושלמו, הסרת סימון מתיבת הסימון מחילה את ה-GPO לכל המשתמשים שלהם הוקצתה הרשאת Apply Group Policy.

Deleting the Default Domain Policy

כברירת מחדל, ה-Default Domain Policy GPO לא ניתן למחיקה על ידי Administrator כלשהו. זאת כדי למנוע מחיקה בשוגג של GPO, המכיל הגדרות חשובות ונדרשות עבור ה-Domain. אם ה-Default Domain Policy לא תיושם, לדוגמה, כיון שהמדיניות יושמה על ידי GPO אחר, סמן את תיבות הסימון Disable Computer Configuration Settings, ו- Disable User Configuration Settings בתיבת הדו-שיח Properties של Default Domain Policy. תוכל גם לסמן את תיבת הסימון Block Policy Inheritance עבור GPO נמוך יותר בהירכיה, כך שה-Default Domian Policy לא תהיה ישימה. כל זה יפעל כל עוד ה-GPO ההורה אינו מוגדר באפשרות No Override Link.

תמיכה במערכות Windows 95, Windows 98 ו-Windows NT 4.0

תוסף התוכנה Group Policy אינו מספק תמיכה למחשבי Windows 95, Windows 98 ו-Windows NT.

תמיכה בלקוחות Windows NT 4.0 ניתנת על ידי תמיכה מלאה בתבניות הניהול מסוג Windows NT 4.0 (קבצי adm) ואספקת קבצי System Policy (שנוצרו על ידי Poledit.exe) של Windows NT 4.0. עורך System Policy של Windows 9x עדיין ישמש לניהול לקוחות Windows 95 ו-Windows 98.

לקוחות הפועלים תחת מערכות Windows 95 ו-Windows 98, צריכים להעתיק את הקובץ Config.pol שנוצר במערכת ההפעלה של מחשב הלקוח לתיקיית שיתוף Netlogon של ה-domain.

לקוחות Windows NT 4.0 משתמשים בקובץ Ntconfig.pol, שהם קוראים בעת ההתחברות לרשת. ברשת Windows NT Server, שם שיתוף ההתחברות הוא Netlogon והוא ממוקם בתיקיה %systemroot%\System32\Rep\Import\Scripts. שיתוף Netlogon לרשת עבור Windows 2000 ממוקם בתיקיה %systemroot%\SYSVOL\Sysvol\<**DomainName.com**>\Scripts. מחשבי לקוח Windows 95, Windows 98, ו-Windows NT, יחפשו שיתוף זה לאיתור הקובץpol. היחסי שלהן.

למידע אודות התקנת System Policy Editor (עורך מדיניות המערכת), עיין בעזרה של Windows 2000 Server. עורך מדיניות המערכת כלול ב-Windows 2000 Server, אך לא ב-Windows 2000 Professional. חבילת Windows 2000 Optional Administrative Tool

Pack (Adminpak.msi), הכוללת את System Policy Editor נמצאת על תקליטור ההתקנה של Windows 2000 Server עבור מחשבים המריצים Windows 2000 Professional. Adminpak.msi אינו מציג רכיב תוכנה בקבוצה Administrative Tools. להפעלת עורך המדיניות של Windows NT, הקלד **poledit** בתיבת הדו-שיח Run.

ניהול Group Policies

לאחר שהגדרת את אובייקטים מדיניות הקבוצה שלך, ואם רצית, הגדרת MMC Console הכולל תוסף תוכנה Group Policy עבור כל GPO, אתה מוכן לנהל את מדיניות הקבוצה.

ניהול הגדרות תוכנה

השתמש בתוסף התוכנה Group Policy לנהל הפצת תוכנה בצורה ריכוזית. תוכנה ניתן להתקין, להקצות, לפרסם, לעדכן, לתקן, ולהסיר התקנה עבור קבוצות, משתמשים ומחשבים.

לפני השימוש בתוסף התוכנה Group Policy להפצת תוכנה, יש לרכוש חבילות התקנת תוכנות (msi.) Microsoft Windows Installer עבור התוכנות. ניתן לרכוש חבילות התקנה בדרכים הבאות:

- ספק התוכנה או המפתח עשויים לספק את חבילות Microsoft Windows Installer עבור יישומיהם. לדוגמה, מוצרי מיקרוסופט כוללים חבילות התקנה של Windows Installer. ספקי צד שלישי של כלי התקנת תוכנה יספקו חבילת Windows Installer עבור התוכנות שלהם.
- ה-Administrator יכול להשתמש בכלי Package ליצור מארז Windows Installer. ספקי צד-שלישי של כלי התקנת תוכנה יכולים לספק ל-Administrators כלי Package של Windows Installer הדרושים להם לצורך אריזה מחדש של התוכנות שלהם.

הקצאה ופרסום של יישומים

ניתן להקצות (Assigned) יישומים עבור משתמשים ומחשבים, ולפרסם (Published) יישומים עבור המשתמשים.

הקצאה למשתמשים

בעת הקצאת יישום למשתמש, היישום מודיע למשתמש על קיומו בפעם הבאה שהוא יתחבר לתחנת עבודה. הודעת היישום עוקבת אחר המשתמש בלי תלות באיזה מחשב פיסי הוא משתמש בפועל. היישום מותקן כאשר המשתמש טוען את היישום למחשב לראשונה, או על ידי בחירת היישום בתפריט Start, או על ידי הפעלת מסמך הקשור ליישום (כגון מסמך DOC אשר עשוי להתקין את יישום Winword).

הקצאה למחשבים

כאשר מקצים (Assigned) יישום למחשב, ההתקנה מתרחשת אוטומטית בעת הפעלת המחשב והמשתמש אינו יכול להסיר אותה.

פרסום למשתמשים

בעת פרסום של היישום למשתמשים, היישום נראה כלא מותקן על מחשבי המשתמשים. אין קיצורי דרך על שולחן העבודה או בתפריט התחלה, ולא מתבצעים שינויים ברישום המקומי של מחשבי המשתמשים. במקום זאת, יישומים שפורסמו שומרים את אפיוני הפרסום שלהם ב-Active Directory. אז, נתונים כמו שם היישום ושיוך קבצים נחשפים למשתמשים במכולה Active Directory. היישום עתה זמין להתקנה באמצעות היישומון Add/Remove Programs שבלוח הבקרה, או על ידי לחיצה על קובץ המשויך ליישום (כגון קובץ xls. ב-Microsoft Excel).

הקצאה ופרסום של יישומים

להקצאה או פרסום של יישום, צור תיקיה משותפת והעתק את קבצי היישום וקבצי המארז (קבצי msi.) לתיקיה המשותפת. הקצה את ההרשאות הבאות לתיקיה המשותפת:

- Everyone=Read
- Adminstrators=Full Control

להקצאה או פרסום של יישום, פתח את תוסף התוכנה Group Policy עבור ה-GPO המתאים, ובחר את תת התיקיה Software Settings\Software Installation מ-Computer Configuration או User Configuration. מתפריט Action, בחר New ובחר Package. עיין עד שתגיע לשיתוף הרשת שיצרת, ובחר את החבילה שיש להקצות. תופיע תיבת דו-שיח Deploy Application. בחר שיטת הפצה.

לחץ על Assigned: Deployed To All Users At Logon, או לחץ Published: Users Install Via Add/Remove Programs Wizard, ולחץ OK. שם היישום שיש ליישמו או לפרסמו, בנוסף לתכונות נוספות עבור היישום, יופיע בחלונית הפרטים.

הטבלה להלן מתארת כיצד יישומים מופצים:

אם היישום...	בצומת זה	הוא מופיע ב...
הוקצה Assigned	תצורת משתמש User Configuration	בתפריט Start, עבור כל **המשתמשים** באתר, Domain או OU.
	תצורת מחשב Computer Configuration	בתפריט Start, עבור כל **המחשבים** באתר, Domain או OU.
פורסם Published	תצורת משתמש User Configuration	אשף Add/Remove Programs עבור כל **המשתמשים** ב-Site, Domain, OU.

Managing Scripts

מדיניות הקבוצה של Windows 2000 מאפשרת גמישות ניכרת בעת הקצאת תסריטים (Scripts). ניתן להקצות תסריטי הפעלה וכיבוי למחשבים, אשר Windows 2000 מעבדת כאשר היא מאתחלת או נכבית. כמו כן ניתן להקצות תסריטי התחברות וניתוק למשתמשים, ש- Windows 2000 מעבדת בעת התחברות או התנתקות משתמש.

Windows 2000 מפעילה תסריטים כדלקמן:

- ❖ בעת הקצאת תסריטים רבים להפעלה וכיבוי, או התחברות והתנתקות למחשב או משתמש, Windows 2000 מבצעת את התסריטים מלמעלה למטה. ניתן לקבוע את סדר הביצוע עבור ריבוי-תסריטים בתיבת הדו-שיח Properties.
- ❖ כאשר מכבים מחשב, Windows 2000 מעבדת תחילה תסריט התנתקות ולאחר מכן תסריטי כיבוי. ברירת המחדל של זמן ביטול הביצוע (Timeout) לעיבוד תסריטים הוא שתי דקות. אם תסריטי ההתנתקות והכיבוי אורכים יותר משתי דקות, עליך לכוון את זמן הביטול באמצעות מדיניות תוכנה.

הערה Windows 2000 מאחסנת תסריטים בתיקית התסריטים של GPT.

תוסף התוכנה Group Policy ב-Windows 2000 מאפשר גמישות ניכרת בעת החלת תסריטים. Administrators יכולים להקצות תסריטי התחברות והתנתקות למחשבים כמו גם תסריטי התחברות והתנתקות למשתמשים. תסריטים מתוזמנים לפעול עקב אירוע מסוים Startup/Shutdown למחשבים, ו-Logon/Logoff עבור משתמשים. כפי ששמם מעיד, התסריט מעובד עם אתחול או כיבוי מערכת ההפעלה, או כאשר המשתמש מתחבר או מתנתק.

התסריטים (Scripts) הניתנים לשימוש יכולים להיות קבצי אצווה של Windows NT (.bat או .cmd), קבצי VBScript (.vbs), או קבצי JScript (.js) עם Windows Scripting Host.

להקצאת תסריטים, לחץ לחיצה כפולה על סמל התסריט המתאים (Startup, Shutdown, Logon, Logoff) ולחץ Add. עיין עד לתסריט שברצונך ליישם. לאחר בחירת התסריט, הוסף פרמטרים לשורת הפקודה עבור התסריט.

Multiple Scripts

ניתן להקצות תסריטי התחברות/התנתקות או אתחול/כיבוי רבים למשתמש, או למחשב. בעת שימוש בתסריטים מרובים השתמש בלחצנים מעלה/מטה, בתיבת הדו-שיח Properties, כדי לקבוע את סדר הפעלתם. התסריטים יתבצעו לפי הסדר, מלמעלה למטה.

Show Files

לחיצה על לחצן Show Files, תפתח חלון שיציג את תכולת תיקית התסריטים המתאימה. בכך, מתאפשרת צפייה בתסריטים וקבצים משויכים הקיימים עבור GPO זה.

ניהול הגדרות אבטחה

מדיניות אבטחת המחשב עוסקת במספר נושאי מדיניות, ניהול זכויות והרשאות משתמשים.

שני סוגים של מדיניות אבטחה מוגדרים במערכת Windows 2000 :

- מדיניות אבטחת Domain.
- מדיניות אבטחת מחשב (ידוע גם כאבטחה מקומית).

מחשב שאינו חלק מ-Windows 2000 Domain, מושפע רק ממדיניות אבטחת מחשב. מחשב שהוא חבר ב-Windows 2000 Domain, מדיניות אבטחת מחשב מיושמת עליו תחילה, ולאחריה מדיניות אבטחת domain.

Windows 2000 מספקת את התשתית להגדרת וניהול מדיניות אבטחה זו בצורה מרכזית ולהחלת אכיפה על כל המחשבים ב-Domain.

תשתית האבטחה ניתנת להפרדה למספר קטגוריות:

- **Account Policies** (מדינויות חשבונות) – קטגוריה זו מאפשרת הגדרת אבטחה למדיניות סיסמאות, מדיניות נעילה, ומדיניות Kerberos ב-Windows 2000 Domains.
- **Local Policies** (מדינויות מקומיות) – קטגוריה זו מאפשרת הגדרת אבטחה ליומני האירועים של היישומים, אבטחה ומערכת. ניתן לגשת ליומנים אלה באמצעות מציג האירועים (Event Viewer) וכן הגדרת זכויות ומדיניות אבטחה.
- **Restricted Groups** (קבוצות מוגבלות) – קטגוריה זו מאפשרת הגדרת מי צריך ומי לא צריך להשתייך לקבוצה מוגבלת, כמו גם לאיזה קבוצות צריך לשייך קבוצות מוגבלות. הגדרות אלו מאפשרות ל-administrators לאכוף מדיניות אבטחה על קבוצות רגישות, כגון Enterprise Administrators או Payroll. לדוגמה, ניתן להחליט שרק Joe ו-Mary יהיו חברים בקבוצה Enterprise Administrators. קבוצות מוגבלות יכולות לשמש לאכיפת מדיניות זו. אם משתמש שלישי מתוסף לקבוצה (לדוגמה, כדי לבצע מטלה כלשהי במצב חירום), בפעם הבאה שהמדיניות נאכפת, המשתמש השלישי מוסר אוטומטית מהקבוצה Enterprise Administrators. המדיניות חוזרת ומיושמת כל 90 דקות כברירת מחדל. לכן, למשתמש השלישי יהיה זכויות Enterprise Administrator לתשעים דקות לכל היותר.
- **System Services** (שירותי מערכת הפעלה) – קטגוריה זו מאפשרת הגדרת מצב האתחול ואפשרויות אבטחה (Security Descriptors) לשירותי מערכת הפעלה כגון שירותי רשת, שירותי קבצים והדפסות, שירותי טלפון ופקס, שירותי אינטרנט ואינטראנט וכו'.
- **Registry** (רישום המערכת) – קטגוריה זו מאפשרת הגדרת אבטחה למדיניות עבור מפתחות הרישום, כולל בקרת גישה, בחינה ובעלות. בעת החלת אבטחה על מפתח רישום, הרחבת Security Settings עוקבת אחר שיטת הירושה בצורה זהה לזו המשמשת את כל ההיררכיות במבנה-עץ של Windows 2000 (כגון Active Directory ו-NTFS). Microsoft ממליצה שתשתמש ביכולות הירושה להגדרת אבטחה רק עבור אובייקטים ברמה הגבוהה ביותר, ולהגדיר מחדש אבטחה רק עבור הצאצאים הדורשים זאת. גישה זו מפשטת מאד את מבנה האבטחה ומפחיתה את עלויות הניהול, שהן תוצאה של מערכת מורכבת ללא לצורך של בקרת גישה.

- ❖ **File System** (מערכת קבצים) – קטגוריה זו מאפשרת הגדרת אבטחה עבור אובייקטים של מערכת קבצים, כולל בקרת גישה, בחינה ובעלות.
- ❖ **Public Key Policies** (מדיניות מפתח ציבורי) – קטגוריה זו מאפשרת הגדרת סוכני אחזור מידע מוצפנים, Auto-Enrollment (מדיניות הצטרפות אוטומטית), Domain roots, ו- Trusted Certificate Authorities.
- ❖ **IP Security Services On Active Directory Services** (מדינות אבטחת IP ב- Active Directory Services) – קטגוריה זו מאפשרת הגדרת אבטחת IP ברשת.

ערכה של תבניות אבטחה מוגדרות מראש מאוחסנת בתיקיה %systemroot%\Security\Templates. תצורות אבטחה מוגדרות-מראש אלו יכולות לשמש כבסיס להגדרות אבטחה, ואז ניתן לערכן בהתאם לצרכי הארגון שלך.

תצורות אבטחה מאוחסנות כקבצי inf בפורמט טקסט המכונה SDDL - **S**ecurity **D**escriptor **D**efinition **L**anguage. בעת הקצאה או עריכת תצורת אבטחה, קובץ התצורה מעובד, והשינויים המתאימים מבוצעים למחשבים או חשבונות המשתמשים המשויכים.

ניהול Administration Templates

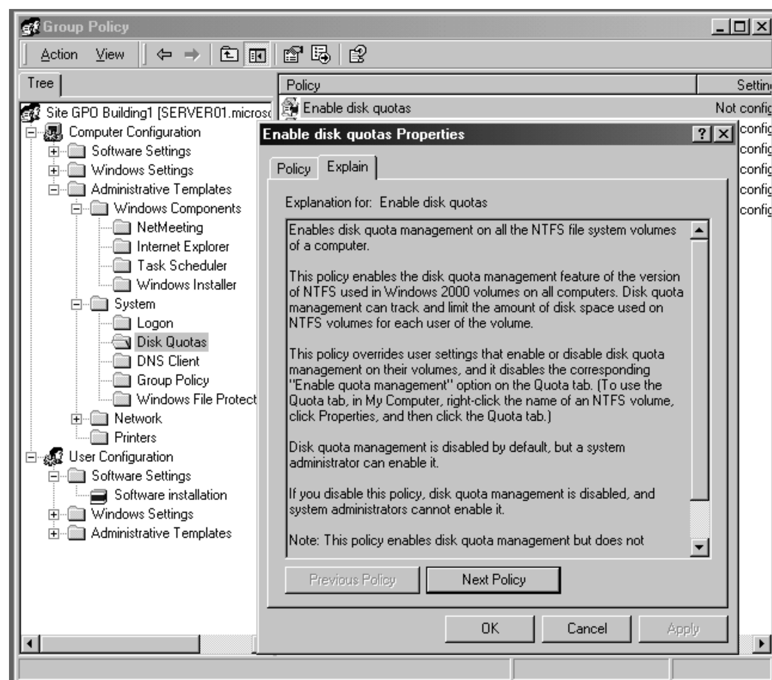
במערכת Windows 2000, הרחבת Administrative Templates בתוסף התוכנה Group Policy, משתמש בקובץ תבנית ניהולית (adm) לציון הגדרות התבנית הניתנות לשינוי באמצעות תוסף התוכנה Group Policy. כל מדיניות מספקת רשימת הגדרות מדיניות המוחלות ל-Site, Domain או OU.

המדיניות שתחת Administrative Templates מייצגות הגדרות Registry-based group policy. Administrative Templates מכתיבות מיגוון התנהגויות של מערכת ההפעלה של Windows 2000, רכיביה ויישומיה. הגדרות אלה נכתבות לחלק HKEY_CURRENT_USER (HKCU), או HKEY_LOCAL_MACHINE (HKLM) של הרישום, כנדרש.

קובץ adm הוא קובץ טקסט Unicode (תמיכת Unicode עבור קבצי adm חדשה ל-Windows 2000). הקובץ מגדיר היררכיה של קטגוריות ותת-קטגוריות שמגדירות ביחד את תצוגת האפשרויות. כמו כן היא מציינת את המיקומים ברישום המערכת בהם נדרש לבצע שינויים עבור בחירה מסוימת, מגדירה אפשרויות והגבלות (כערכים) המשויכות לבחירה, ובמקרים מסוימים, מגדירה ערך ברירת מחדל לשימוש במידה ובחירה כלשהי מופעלת.

הכרטיסיה Explain שבכל תיבת דו-שיח Properties כוללת פרטים על הגדרות המדיניות בקובץ adm. תרשים 7.16 מראה את הכרטיסיה של System Policy.

הצומת Administrative Templates של תוסף התוכנה Group Policy ניתן להרחבה על ידי שימוש בקבצי adm מותאמים באופן אישי.



תרשים 7.16 הכרטיסיה Explain עבור מאפיין המערכת Enable Disk Quatas.

הגדרות רישום מתמידות

הגדרות Registry במערכת Windows NT 4.0 תקפות, כל עוד הן אינן מבוטלות באופן מוחלט. התנהגות זו נקראת Tattooing (קעקוע). בניגוד לכך, הגדרות הרישום של Windows 2000, נמחקות ונכתבות מחדש בכל פעם שמשתנה המדיניות. אם אתה מורגל במדיניות הגדרת רישום המערכת של Windows NT 4.0, הייה מודע להתנהגות זו.

ניהול Folder Redirection

הרחבת Folder Redirection מאפשרת ניתוב כל אחת מהתתיקיות המיוחדות הבאות שבפרופיל משתמש למיקום חליפי (כגון שיתוף רשת):

- Application Data
- Desktop
- My Documents
- My Documents\My Pictures
- Start Menu

לדוגמה, ניתן לנתב את התיקיה My Documents של משתמש מסוים לנתיב \\<server>\<share>\%username%. על ידי ניתוב התיקיה My Documents, ניתן לקבל את היתרונות הבאים:

- וידוא שמסמכי המשתמש זמינים בכל מחשב ברשת.
- הפחתת זמן ההתחברות וההתנתקות מהרשת. במערכת Windows NT 4.0, התיקיה My Documents היא חלק מפרופיל משתמש נודד (RUP). המשמעות היא שהתיקיה My Documents על תכולתה מועתקים הלוך וחזור בין מחשב הלקוח והשרת בעת התחברות והתנתקות משתמשים. העברת התיקיה My Documents מחוץ לפרופיל המשתמש יכולה להפחית זמן זה באופן משמעותי.
- אחסון נתוני משתמשים ברשת (ולא על המחשב המקומי). כך ניתן לנהל את הנתונים בצורה מרוכזת, ולהגן עליהם באמצעות נוהלי גיבוי רשת ו-Dfs של domains.
- לגרום לתיקיה מבוססת-הרשת My Documents שתהיה זמינה למשתמשים בעת שהם מנותקים מהרשת הארגונית, על ידי שימוש בטכנולוגיות Offline Folders.

כברירת מחדל, הרחבת Folder Redirection אינה כלולה בתוסף התוכנה Group Policy. כדי להשתמש ב-Folder Redirection, עליך ליצור MMC console הכוללת תוסף תוכנה Group Policy עבור כל GPO נתמך. במקום המתאים, הוסף את הרחבת Folder Redirection לתוסף התוכנה Group Policy.

תרגיל 6: יצירת Group Policy Object והגדרת מדיניות

בתרגיל זה, תיצור GPO בשם Domain Policy ל-domain שלך. לאחר מכן תשתמש בתוסף התוכנה Group Policy לשנות את הגדרות האבטחה של ה-GPO, כדי לאפשר לחברים בקבוצה Domain Users להיכנס באופן מקומי ל-DCs. בצע תרגיל זה על שרת Server01.

הליך 1: יצירת GPO

בהליך זה. תיצור GPO (אובייקט מדיניות קבוצתית) ברמת ה-Domain.

1. התחבר ל-domain בשם משתמש Administrator עם הסיסמה Password.
2. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ Active Directory Users And Computers. תוסף התוכנה Active Directory Users And Computers יופיע.
3. לחץ על microsoft.com בחלון Tree, פתח את תפריט Action, ולחץ Properties. תיבת הדו-שיח Properties של microsoft.com תופיע.

4. בחר בכרטיסיה Group Policy, ולחץ Add. תיבת הדו-שיח Add A Group Policy Object Link תופיע.

5. בחר בכרטיסיה All. שים לב שברשימה מופיע Default Domain Policy. ניתן להשתמש ב-GPO זה ולשנותו כנדרש, אך לצורך הליך זה, תיצור GPO חדש ל-Domain.

6. לחץ על הלחצן האמצעי מבין שלושה שעל סרגל הכלים. GPO חדש בשם New Group Policy Object יופיע ברשימת Group Policy Objects.

7. תן ל-GPO את השם **Domain Policy**, ולחץ OK. GPO בשם Domain Policy יופיע עתה בעמודה Group Policy Object Links.

8. לחץ OK לסגירת תיבת הדו-שיח Group Policy Properties.

9. השאר את תוסף התוכנה Active Directory Users And Computers פתוח.

הליך 2: שינוי הגדרות אבטחה

בהליך זה, תשתמש ב-Group Policy Editor לשינוי הגדרות האבטחה, כדי לתת לקבוצה Domain Users את הזכות להיכנס באופן מקומי לשרת Server01.

1. בחלון Tree, הרחב את microsoft.com.

2. לחץ על המכולה Domain Controllers.

3. פתח את תפריט Action, ואז את תפריט Properties. תיבת הדו-שיח Domain Controllers Properties תופיע.

4. בחר בכרטיסיה Group Policy.

5. ברשימה Group Policy Object Links, ודא ש-Default Domain Controllers Policy מואר, ולחץ Edit.

6. יופיע תוסף התוכנה Group Policy ויוצג בחלון Default Domain Controller - Tree Policy.

7. בחלון Tree, ודא שהצומת Computer Configuration, הורחב.

   יופיעו מדינויות Computer Configuration.

8. הרחב Windows Settings מתחת לצומת Computer Configuration. מדיניות Windows Settings תופיע.

9. הרחב Security Settings מתחת לצומת Window Settings.

   מדיניות Security Settings תופיע.

10. הרחב Local Policies מתחת לאובייקט Security Settings. יופיע Local Policies.

11. לחץ על User Rights Assignment מתחת לאובייקט Local Policies. רשימת אפיוני הקצאות זכויות משתמשים תופיע בחלונית הפרטים.

12. לחץ לחיצה כפולה על Log On Locally (התחבר/היכנס באופן מקומי) בחלונית הפרטים. תיבת הדו-שיח Log On Locally תופיע. שים לב שהגדרת מדיניות זו מוקצית למספר אובייקטים של משתמשים וקבוצות.

13. לחץ Add. תיבת הדו-שיח Add Users Or Groups תופיע.

14. לחץ Browse. תיבת הדו-שיח Select Groups Or Users תופיע.

15. ברשימה Names, בחר Domain Users, לחץ Add, ולחץ OK.

טיפ אם אתה מתקשה לאתר את הקבוצה Domain Users, פשוט הקלד **Domain Users** ותכונת השלמת ההקלדה של Windows תאתר את הקבוצה עבורך.

---

16. לחץ OK שנית. Domain Users יופיע ברשימת המשתמשים והקבוצות עם הזכות להתחבר באופן מקומי.

17. לחץ OK, וסגור את תוסף התוכנה Group Policy.

18. לחץ OK לסגירת תיבת הדו-שיח Domain Controllers Properties.

19. השאר את תוסף התוכנה Active Directory Users And Computers פועל, כיון שתשתמש בו בתרגיל הבא.

כל משתמשי ה-domain יכולים עתה להתחבר/להיכנס לשרת Server01 באופן מקומי.

תרגיל 7: שינוי מדיניות תוכנה

בתרגיל זה, תיצור, ולאחר מכן תשנה, את מדיניות ה-OU בשם Sales, על ידי הסרת פריט Search ופריט Run מתפריט Start. כמו כן, תבטל את המדיניות Lock Workstation. לאחר מכן תבחן השפעות של שינויי מדינויות תוכנה אלו. בחלק האחרון של תרגיל זה, תמנע מה-OU בשם Sales לדרוס את מדיניות הקבוצה של מכולת ההורה שלו - ה-Domain. בצע תרגיל זה על שרת Server01.

הליך 1: שינוי מדיניות תוכנה

בהליך זה, תיצור ולאחר מכן תשנה מדיניות תוכנה עבור Sales OU. יצרת את Sales OU בפרק קודם.

1. בתוסף התוכנה Active Directory Users And Computers, הרחב את microsoft.com.
2. בחלון Tree, לחץ Sales, פתח את תפריט Action, ואז לחץ Properties.

   תיבת הדו-שיח Sales Properties תופיע.
3. בחר בכרטיסיה Group Policy.
4. לחץ Add. תיבת הדו-שיח Add A Group Policy Link תופיע.
5. בחר בכרטיסיה All, ולחץ על הלחצן האמצעי מבין השלושה שעל סרגל הכלים.

   GPO חדש יופיע תחת Group Policy Objects Associated With This Container.
6. תן שם **SalesSoftware** ל-GPO חדש זה. אתה מוחזר לכרטיסיה Group Policy של תיבת הדו-שיח Sales Properties.
7. בעוד SalesSoftware מואר, לחץ Edit. תוסף התוכנה Group Policy יופיע.
8. אתר והרחב את Administrative Templates שתחת User Configuration.
9. בחלון Tree, לחץ Start Menu ו- Start Bar. המדיניות הזמינה לקטגוריה זו מופיעה בחלונית הפרטים.
10. בחלונית הפרטים, לחץ לחיצה כפולה על Remove Search Menu From Start Menu.

    תיבת הדו-שיח Remove Search Menu From Start Menu Properties תופיע.
11. לחץ על Explain לקרוא על מדיניות זו.
12. בחר בכרטיסיה Policy ולחץ על לחצן אפשרויות Enabled.
13. לחץ OK.
14. חזור על שלבים 10 עד 13 כדי לאפשר מדיניות Remove Run Menu From Start Menu.

15. בחלון Tree, לחץ לחיצה כפולה על System ולחץ Logon/Logoff. המדיניות הזמינה לקטגוריה זו תופיע בחלונית הפרטים.

16. בחלונית הפרטים, אפשר מדיניות Disable Lock Computer.

17. סגור את תוסף התוכנה Group Policy, וסגור את תיבת הדו-שיח Sales Properties.

18. סגור את תוסף התוכנה Active Directory Users And Computers.

הליך 2: בחינת מדיניות תוכנה

בהליך זה, תצפה בהשפעות של מדיניות התוכנה שיישמת בהליך הקודם.

חשוב לביצוע התרגילים בפרק זה ובפרק 6 צריך שיהיו לך שני חשבונות משתמשים ב-OUs: Sales - Jane Doe ו- John Smith.

---

1. התנתק משרת Server01 כ-administrator.

2. לחץ Ctrl+Alt+Delete.

3. תיבת הדו-שיח של אבטחת Windows 2000 תופיע. שים לב שלחצן Shutdown אינו זמין. מצב זה מופעל על ידי מדיניות Shutdown Without Logon. שים לב שמערכת Windows 2000 Server אינה גורמת שלחצן זה יהיה זמין כברירת מחדל.

4. התחבר לשרת Server01 כ- Jane_Doe עם הסיסמה student.

5. לחץ Start. שים לב שפריטי התפריט Search ו-Run אינם מופיעים בתפריט Start.

הליך 3: מניעת דריסה של מדיניות קבוצה

בתרגיל זה, תמנע מה-Salse OU לדרוס את מדינות הקבוצה של מכולת ההורה שלה.

1. התחבר ל-domain בשם משתמש Administrator עם הסיסמה Password.

2. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על תוסף התוכנה Active Directory Users And Computers.

   חלון תוסף התוכנה Active Directory Users And Computers יופיע.

3. הרחב את microsoft.com.

4. לחץ Sales, פתח את תפריט Action, ולחץ Properties.

   תיבת הדו-שיח Sales Properties תופיע.

5. בחר בכרטיסיה Group Policy.

6. ודא ש- SalesSoftware מואר ברשימת Group Policy Objects Link List, ולחץ Options.

7. לחץ וסמן את תיבת הסימון No Override: Prevents Other Group Policy Objects From Overriding Policy Set In This One, ולחץ OK.

8. לחץ OK שנית, וסגור את תוסף התוכנה Active Directory Users And Computers.

סיכום שיעור

מדינויות קבוצה הן אוסף הגדרות תצורה החלות על אובייקט אחד או יותר במחסן Active Directory. הן משמשות לבקרה על סביבות העבודה של משתמשים באתרים, תחומים או משתמשים השייכים ליחידות ארגוניות מסוימות. יש סוגים רבים של מדיניות קבוצה, כולל הגדרות תוכנה, תסריטים, הגדרות אבטחה, תבניות ניהול, וניתוב תיקיות. מבנה מדיניות קבוצה מורכב מאובייקטים של מדיניות קבוצה, מכולות, ותבניות. לפני שתוכל ליצור מדיניות קבוצה, עליך ליצור אובייקטים של מדיניות קבוצה. משם, תוכל לערוך מדיניות קבוצה על ידי שימוש בתוסף התוכנה Group Policy או לנהל הרשאות באמצעות תוסף התוכנה Active Directory Users And Computers. ניהול מדיניות קבוצה כולל ניהול הגדרות תוכנה, תסריטים, הגדרות אבטחה, תבניות ניהול וניתוב תיקיות.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות לשאלה, עיין בשיעור המתאים ונסה לענות על השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

1. When you use the Administrative Tools program group to open an MMC console provided with Windows 2000 Server, can you add snap- ins to it? Why or why not?
2. You receive a call from a member of the Help Desk support team. She tells you that a number of users are complaining of a window that appears every time they log on. The support person tells you there is nothing in the Startup menu. Additionally, she has closed the window and shut down and restarted the computer, but the window still appears at logon. What is the most likely cause of this issue, and how can you resolve it?
3. When should you use security groups instead of distribution groups?
4. What are the implications of changing the domain mode from Mixed mode to Native mode?
5. By default, in what order is group policy implemented through the Active Directory store hierarchy? How can you control this behavior?
6. What is a GPO, GPC, and GPT?

1. כאשר אתה משתמש ב- Administrative Tools לפתיחת MMC Console המסופקת עם Windows 2000 Server, האם ניתן להוסיף לה תוספי תוכנה? נמק.

2. אתה מקבל קריאה מחבר בצוות התמיכה. נאמר לך שמספר משתמשים מתלוננים על חלון שמופיע להם בכל פעם שהם מתחברים. צוות התמיכה מבהיר לך שאין מאומה בתפריט Startup. בנוסף, המשתמש סגר את החלון, כיבה את המחשב ואתחל אותו שנית, אך החלון עדיין מופיע בעת ההתחברות. מה יכולה להיות הסיבה לתופעה זו, ואיך ניתן לתקנה?

3. מתי יש להשתמש בקבוצות אבטחה במקום קבוצות הפצה?

4. מהן המשמעויות וההשפעות של שינוי מצב ה-Domain מ-Mixed Mode ל- Native Mode?

5. כברירת מחדל, באיזה סדר מיושמת מדיניות קבוצה דרך היררכיית מחסן Active Directory? כיצד ניתן לשלוט על התנהגות זו?

6. מה הם GPO, GPC ו-GPT?

פרק 8

ניהול שירותי הדפסה

אודות פרק זה

פרק זה דן בנושא הגדרת מדפסות ברשת, כך שמשתמשים יוכלו להדפיס באמצעות הרשת. כמו כן דן הפרק בהדפסה מבוססת Active Directory, וכיצד להתחבר למדפסות רשת. הפרק מספק מידע כיצד לאתר תקלות הדפסה נפוצות הקשורות בהגדרת מדפסות רשת.

לפני שתתחיל

לביצוע השיעורים בפרק זה נדרש :

- ❖ מחשב ובו מותקן ופועל שרת Microsoft 2000.
- ❖ שירותי Active Directory מותקנים ופעילים בשרת.
- ❖ השלמת כל התרגילים בפרקים קודמים.

הערה אין צורך במדפסת כדי להשלים את התרגילים בפרק זה.

שיעור 1: מבוא להדפסה בסביבת Windows 2000

שרת Microsoft Windows 2000 נועד להיות גם שרת הדפסה. תוך שימוש במיגוון מערכות, יכולים יישומים לשלוח משימות הדפסה למדפסות המחוברות לשרת Windows 2000, או למדפסות המחוברות לרשת (המדפסות הן חלק מהרשת כמו כל תחנת עבודה אחרת) על ידי כרטיס רשת חיצוני/פנימי (התקני שרת הדפסה), או למדפסות המחוברות פיזית לשרת אחר. על ידי שימוש בשרת Windows 2000 כשרת ההדפסה של הרשת, ניתן להדפיס מכל מחשב ברשת בו פועלת מערכת הפעלה נתמכת. בראשיתו של הפרק תכיר את המונחים המשמשים בשירותי ההדפסה. הפרק יספק לך קווים מנחים להגדרה נכונה של סביבת הדפסה ברשת. כמו כן סוקר פרק זה את הנושאים הקשורים בהדפסה מקומית או מרוחקת, ובהתקני הדפסה המחוברים למחשב ישירות, או באמצעות הרשת.

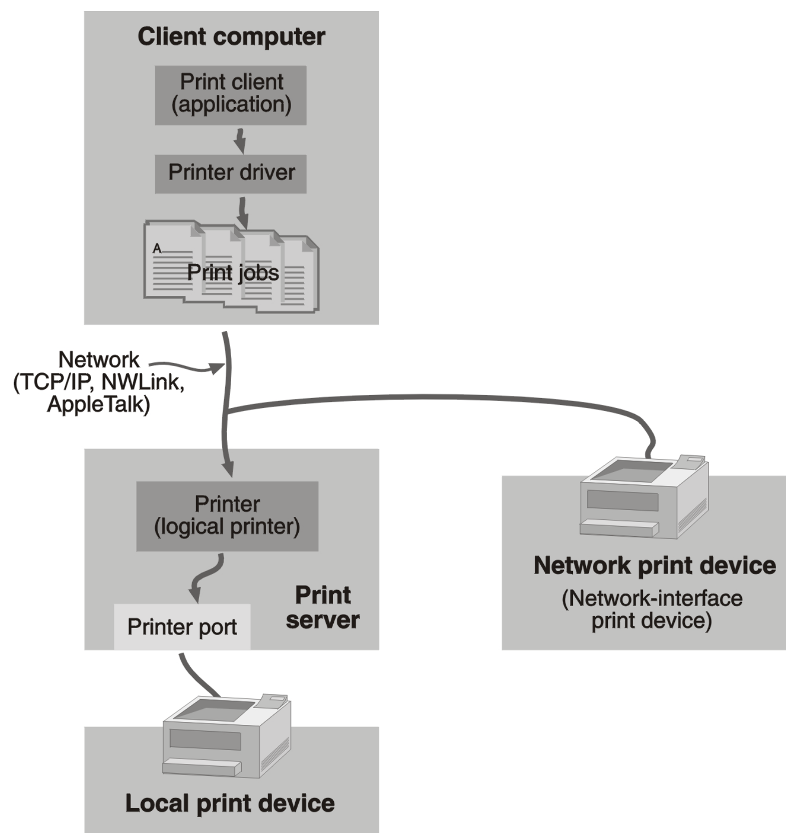
לאחר שיעור זה תוכל

- להגדיר את המונחים הקשורים להדפסה בסביבת Windows 2000
- להגדיר את הדרישות וההנחיות להדפסה בסביבה מרושתת
- לתאר את תרחישי ההדפסה השונים להדפסה מקומית או מרוחקת עבור התקני הדפסה המחוברים לרשת והתקני הדפסה המחוברים ישירות למחשב

זמן שיעור משוער 35 דקות

מונחים

לפני שתתחיל בהגדרת סביבת ההדפסה, רצוי שתכיר את מונחי ההדפסה בסביבת Windows 2000, כדי להבין כיצד רכיבים שונים משתלבים זה בזה, כמתואר בתרשים 8.1 להלן.



תרשים 8.1 מונחי הדפסה.

אם Windows 2000 חדשה לך, ייתכן שכמה ממונחי ההדפסה יהיו שונים משציפית (למרות שמונחי ההדפסה אינם שונים באופן ניכר מאלה המשמשים ב-Windows NT Server). הרשימה הבאה מציגה כמה ממונחי ההדפסה ב-Windows 2000:

- **Printer** (מדפסת לוגית) - ממשק תוכנה המתווך בין מערכת ההפעלה והתקן ההדפסה (המוכר כ**מדפסת**). מדפסת לוגית קובעת כיצד תעובד עבודת ההדפסה וכיצד היא תנותב ליעדה (ליציאה מקומית או ליציאת רשת, לקובץ או למדפסת משותפת מרוחקת), מתי יישלח המסמך וכיצד היבטים אחרים של תהליך ההדפסה ינוהלו. כאשר משתמשים יוצרים קשר למדפסות, הם משתמשים בשמות מדפסת, המצביעים להתקן הדפסה אחד או יותר. זוהי התוכנה שמנהלת את המדפסת.

* **Print device** (התקן הדפסה, מדפסת) - התקן הדפסה, התקן החומרה המייצר מסמכים מודפסים. Windows 2000 תומכת בהתקני ההדפסה הבאים:

  - **Local Print Devices** (התקני הדפסה מקומיים) - התקנים המחוברים ליציאה פיזית בשרת ההדפסה. התקן הדפסה מקומי מחובר למחשב באמצעות ממשק מקומי, כגון ממשק מקבילי, ממשק טורי מסוג RS-232/422/IRDA, USB, או יציאת SCSI.
  - **Network Print Device** (התקני הדפסה ברשת) - התקנים המחוברים לשרת ההדפסה דרך הרשת, ולא דרך יציאה פיסית. התקני ההדפסה של רשת המכונים גם **Network-interface print devices** (התקני הדפסה של ממשק-רשת), דורשים כרטיסי רשת משלהם והם בעלי כתובות רשת משלהם, או שהם מחוברים לכרטיס רשת חיצוני. התקן הדפסה ברשת הוא צומת ברשת; מחשבים שולחים להתקן ההדפסה משימות הדפסה דרך כרטיס רשת, אשר ייתכן והוא מובנה בהתקן ההדפסה. המדפסת מחוברת ישירות לרשת ולא למחשב ברשת.

* **Print Server** (שרת הדפסה) - מחשב בו שוכנות ה-Printers (מדפסות) המשויכות ל-Print Device (התקני הדפסה) שיכולים להיות Local או Network. שרת ההדפסה מקבל מסמכים ממחשבי הלקוחות ומעביר אותם למדפסת לביצוע. אתה מגדיר ומשתף מדפסות בשרת ההדפסה.

* **Printer Driver** (מנהל התקן מדפסת) - קובץ אחד או יותר, המכיל מידע הדרוש ל-Windows 2000 כדי להמיר הוראות הדפסה לשפת הדפסה מיוחדת, כגון PostScript. המרה זו מאפשרת ל-Print Device להדפיס את המסמך. לכל Print Device יש Printer Driver ייחודי.

דרישות עבור רשת הדפסה

דרישות הגדרת הדפסה ברשת בסביבת Windows 2000 הן:

* מחשב אחד לפחות שישמש כשרת הדפסה. אם שרת ההדפסה אמור לנהל מספר רב של משימות הדפסה כבדות, ממליצה Microsoft על שרת הדפסה ייעודי. המחשב יוכל לפעול בסביבת מערכות ההפעלה הבאות:

  - Windows 2000 Server, שיכולה לנהל מספר רב של קישורים ולתמוך במחשבי-לקוח הפועלים בסביבת מערכות ההפעלה MS-DOS, Windows 9x, Macintosh, UNIX, וגם שירותי הדפסה ולקוחות של NetWare.
  - Windows 2000 Professional, המוגבלת ל-10 קישורים בו-זמנית ממחשבים אחרים לשירותי קבצים והדפסה. היא אינה תומכת במחשבי Macintosh או בלקוחות NetWare, אבל תומכת במחשבי MS-DOS, Windows ו- UNIX.

- כמות מספקת של זיכרון לגישה אקראית (RAM) לעיבוד מסמכים. אם שרת הדפסה מנהל מספר רב של מדפסות, או מספר רב של מסמכים גדולים, צריך שתהיה מותקנת במחשב כמות גדולה הרבה יותר של זיכרון RAM מזו הנחוצה ל- Windows 2000 לביצוע משימותיה השוטפות. אם לשרת הדפסה אין מספיק RAM עבור עומס העבודה שלו, ביצועי ההדפסה יפגעו.
- כמות מספקת של שטח פנוי בכונן הדיסק הקשיח של שרת ההדפסה, כדי להבטיח ש-Windows 2000 תוכל לשמור מסמכים ומידע הדפסה אחר שנשלח לשרת ההדפסה, עד אשר שרת ההדפסה ישלח את המידע להתקן ההדפסה. הדבר חשוב במידה והמסמכים גדולים, או שסביר להניח שתהיינה עבודות הדפסה רבות שימתינו לתורן. לדוגמה, אם 10 משתמשים שולחים, בו זמנית, מסמכים גדולים להדפסה, לשרת ההדפסה חייב להיות מספיק שטח כונן כדי לאחסן את כל המסמכים הנמצאים בתור ההדפסה (Spooler), עד שה-Print Server (שרת ההדפסה) ישלח אותם ל-Printer Device (התקן ההדפסה). אם אין מספיק מקום לשמור את כל המסמכים, יקבלו המשתמשים הודעות שגיאה ולא יוכלו להדפיס.

הערה משימות הדפסה בתור ההדפסה יכולות להיות גדולות בהרבה מן המידע הממשי שיישום ההדפסה (מעבד תמלילים או גיליון אלקטרוני) קורא. זאת מכיון שמשימות הדפסה נשלחות דרך מנהל התקן ההדפסה כדי להכין את המידע עבור המדפסת.

הנחיות לסביבת הדפסה ברשת

לפני שתגדיר הדפסה ברשת, יש לפתח אסטרטגיית הדפסה ברשת שתתאים לדרישות ההדפסה של המשתמשים, תוך הימנעות מכפילות לא נחוצה של משאבים או עיכובים בתהליך ההדפסה. הטבלה הבאה מציגה מספר הנחיות לפיתוח אסטרטגיית הדפסה ברשת:

קו מנחה	הסבר
קבע את דרישות ההדפסה של המשתמשים.	קבע את מספר המשתמשים המדפיסים, ואת עומס העבודה. לדוגמה, 15 אנשים במחלקת גבייה אשר מדפיסים מספר רב של חשבוניות לאורך היום יצרו עומס עבודה גדול ואפשר שידרשו יותר מדפסות (Printers), התקני הדפסה (Print devices) ואולי אף יותר שרתי הדפסה (Print servers), מאשר 15 מתכנתים העושים את עבודתם בצורה מקוונת.
קבע את דרישות ההדפסה של החברה.	קבע את צרכי ההדפסה של החברה. קבע את מספר וסוגי התקני ההדפסה (Print devices) הדרושים. בנוסף, שקול את עומס העבודה המוטל על כל התקן הדפסה (Print device). אל תשתמש בהתקן הדפסה אישי לצורך הדפסה ברשת.

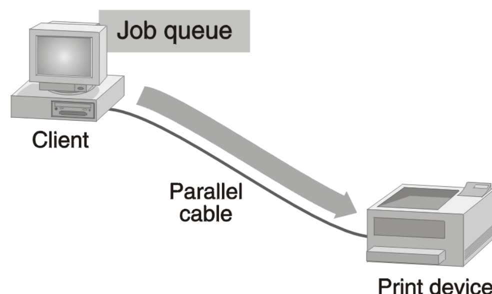
קו מנחה	הסבר
קבע את מספר שרתי ההדפסה הדרושים.	קבע את מספר שרתי ההדפסה הדרושים ברשת, כדי לנהל את מספר וסוגי מדפסות שתוגדרנה ברשת.
קבע היכן יש למקם את התקני ההדפסה (המדפסות).	קבע היכן תמקם את התקני ההדפסה (Print devices). ברשת מנותבת, כדאי למקם את שרת ההדפסה ואת התקני ההדפסה באותה רשת עם מחשבי הלקוח שישתמשו בהם. כך גם יהיה נוח למשתמשים לאסוף את המסמכים המודפסים שלהם.

תצורות הדפסה

בסביבת Windows 2000 ניתן ליצור מיגוון רחב של שילובי לקוחות, שרתים, והתקני הדפסה (Print devices), תלוי אם התקן ההדפסה מרוחק או שאינו מרוחק. הגישה להתקן הדפסה (Print Device) מרוחק היא באמצעות שרת הדפסה. התקן הדפסה שאינו מרוחק מקבל נתונים ישירות מהמחשב. שילוב לקוחות, שרתים והתקני הדפסה תלוי גם בשאלה אם התקן ההדפסה הוא ברשת או שהוא מקושר ישירות למחשב. ברור שכל התקן הדפסה (Print device) מחובר פיזית לרשת או מחובר פיזית לאחד המחשבים שברשת (לאו דווקא לשרת, בהחלט יכול להיות לתחנת עבודה/מחשב שולחני).

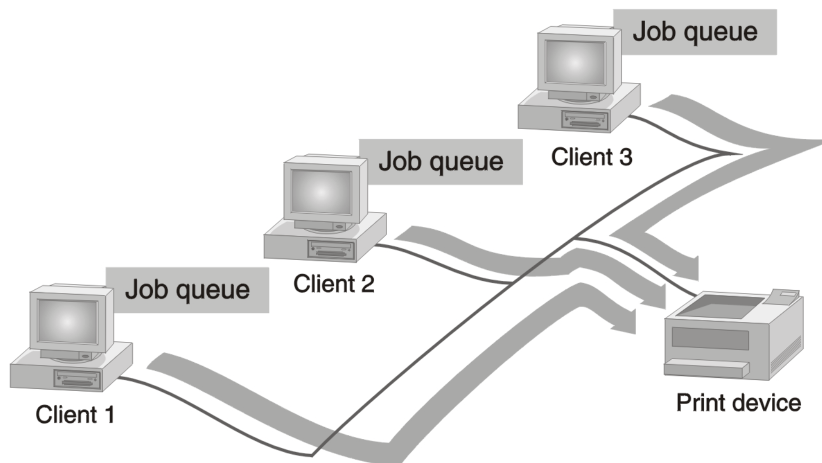
התרשימים הבאים מציגים ארבע תצורות הדפסה בסיסיות. הקווים הדקים מייצגים קישורים פיסיים, כגון רשת או כבלים מקבילים, והחיצים מייצגים את כיוון זרימת המידע.

תרשים 8.2 מציג את התצורה הפשוטה ביותר, התקן הדפסה מקומי (Local Print Device), שאינו מרוחק. התקן ההדפסה מחובר ליציאה המקבילית במחשב המפעיל את היישום. מנהל התקן ההדפסה (Printer Driver) ותור ההדפסה (Spooler ,Job Queue) נמצאים באותו מחשב אשר שולח מידע להדפסה ישירות להתקן ההדפסה (Print Device).



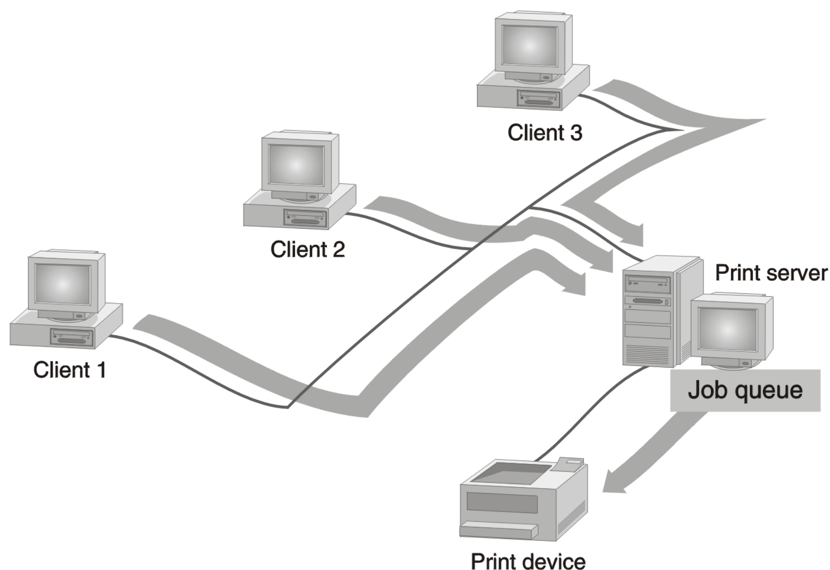
תרשים 8.2 Local Print Device

תרשים 8.3 מציג קבוצה קטנה של מחשבים המשתפים ביניהם Print Device (התקן הדפסה) ברשת (מדפסת רשת). זוהי רשת שיוויונית (Peer-to-Peer), בה לכל מחשב יש גישה שווה להתקן ההדפסה ואין בה בקרה מרכזית או הגנה על ההדפסה. בכל מחשב יש תור הדפסה משלו והוא אינו רואה את המסמכים שבתור ההדפסה במחשבים האחרים. אם ההדפסה נעצרת, הודעת השגיאה אינה מופיעה בכל מחשב לקוח. הדבר נסבל בארגונים קטנים, בהם המשתמשים נמצאים במגע תכוף, אולם הוא מקשה על הניהול ככל שהתנועה ברשת גדלה. התנגשות בין מחשבים השולחים מסמכים להדפסה יכולה לגרום להתקן המדפסת לעצור או לדחות משימות הדפסה.



תרשים 8.3 מדפסת רשת שאינה מרוחקת.

תרשים 8.4 מתאר תצורת רשת המשתמשת בשרת הדפסה מרכזי. הגישה ל-Print Device (התקן ההדפסה) משותפת ללקוחות רבים דרך השרת, אליו מחובר התקן ההדפסה באופן פיסי ישיר באמצעות כבל. תור ההדפסה (Job queue) מוסדר בשרת וגלוי לכל לקוח. כלומר כל מחשב לקוח המחובר לשרת ההדפסה יכול לראות את התור להדפסה בשרת ההדפסה, בין אם הוא שלח מסמך(ים) להדפסה ואם לאוו. מחשב לקוח אינו יכול לבצע פעולות על התור, אפילו על המסמכים שהוא שלח. רק בשרת ההדפסה המחובר ישירות להתקן ההדפסה (Print Device) יש יכולת לנהל את התור: למחוק, להשהות הדפסה וכדומה.

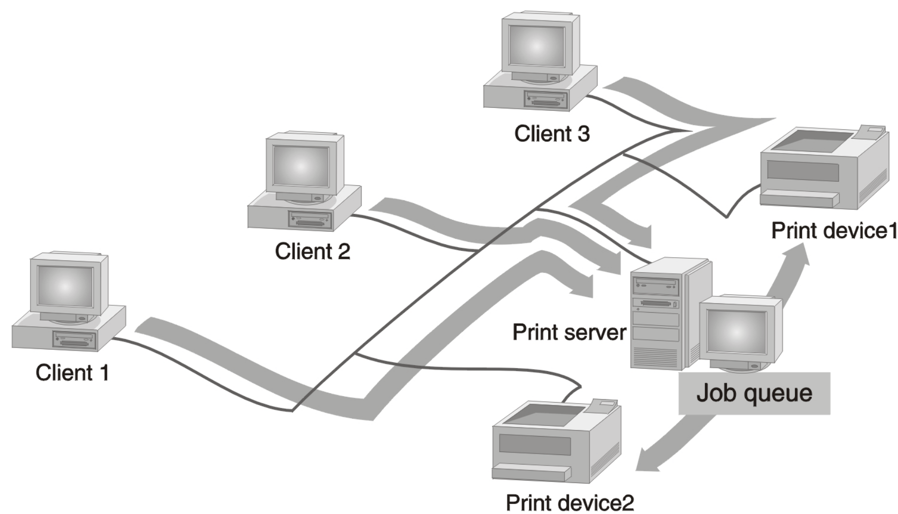


תרשים 8.4 התקן מדפסת מקומי, מרוחק.

ההדפסה מנוהלת על ידי מנהל השרת. המנהל מגדיר וכופה תוכנית הגנה על הרשת, מתחזק את ה-Priner Driver וטוען אותה ללקוחות, כאשר הם מתחברים למדפסת המשותפת. כאשר לקוח שולח הדפסה לתור הדפסה ברשת, הוא מחפש בשרת ההדפסה אחר Printer Driver חדשים, ובמידת הצורך מעדכן את ה-Printer Drivers הישנים שבמחשב שלו (זה קורה רק אם מערכת ההפעלה בשרת ההדפסה היא לפחות Windows NT 4 ומעלה).

לקוחות יכולים להיות מחוברים למספר התקני הדפסה (Print Devices), ובדרך כלל מקושרים לשרת הדפסה אחד מספר התקני הדפסה. מכל מקום, מספר היציאות המקביליות מגביל את מספר התקני ההדפסה שיכולים להיות מקושרים ישירות לשרת ההדפסה.

תרשים 8.5 מראה מספר לקוחות המשתפים ביניהם Print Device ב-Domain הנשלט על ידי מחשב המפעיל Windows 2000 Server; התקן ההדפסה קשור לשרת דרך הרשת (ולא פיזית דרך כבל טורי), ומאפשר לשרת הדפסה אחד לנהל כמה התקני הדפסה.



תרשים 8.5 התקן מדפסת של רשת, מרוחק.

כדי ליצור ולשתף במדפסות השתמש באשף Add Printer. אשף זה נמצא בתיקיה Printers. ניתן לגשת אליו דרך תפריט Start על ידי לחיצה על Settings ולחיצה על Printers. ללא קשר למקום בו ממוקמים התקני ההדפסה (Print Devices), תוכנת המדפסת (Printer) חייבת להיות מותקנת בשרת ההדפסה. אם התקן ההדפסה מחובר ישירות לשרת (באמצעות כבל טורי, לדוגמה), יזהה אותו האשף וינסה להגדיר את תוכנת המדפסת הלוגית (Printer). אם התקן ההדפסה ממוקם במקום אחר כלשהו ברשת, עליך למפות יציאה כשאתה מתקין את המדפסת הלוגית (Printer). תוכל להשתמש באשף Add Printer גם כדי להתחבר להתקני הדפסה מרוחקים. כשתבצע פעולה זו עליך לזכור כי:

- **יצירת מדפסת** משמעותה התקנת התקן הדפסה (Print Device), בין אם ישירות לשרת ההדפסה או התקן הדפסה רשת, והגדרת תוכנת המדפסת הלוגית (Printer) השולטת בתהליך ההדפסה בשרת. הפעל את אשף Add Printer ובחר באפשרות Local Printer (מדפסת מקומית). עליך לתת שם עבור המדפסת, להתקין עבורה את מנהל ההתקן (Printer Driver) התואם ולציין יציאה עבורה (למשל, LPT1).

- **התקשרות למדפסת** משמעותה התחברות למדפסת משותפת ברשת המותקנת על אחד מהמחשבים שברשת. כדי להתחבר למדפסת, הפעל את אשף הוספת המדפסות ובחר באפשרות Network Printer. אם מנהל התקן (Printer Driver) המדפסת עבור סוג מערכת ההפעלה של הלקוח קיים בשרת ההדפסה, אין צורך להתקין אותו, מכיון ש-Windows 2000 מורידה אותו באופן אוטומטי. זה כולל מנהלי התקן (Print Drivers) עבור Windows 9x וכל גרסאות Windows NT. במקרים אחרים, תתבקש לספק את קבצי מנהל ההתקן (Printer Drivers) המתאימים.

סיכום שיעור

מדפסת לוגית (Printer) היא ממשק התוכנה שבין מערכת ההפעלה והתקן ההדפסה (Print Device, המדפסת). התקן הדפסה (המדפסת), הוא התקן החומרה המייצר את המסמך המודפס. שרת הדפסה (Print Server) הוא מחשב בו שוכנות המדפסות הלוגיות (Printers) המשויכות להתקני הדפסה מקומיים או להתקני הדפסה ברשת. מנהל התקן מדפסת (Printer Driver) הוא קובץ אחד או יותר המכיל מידע הנדרש על ידי Windows 2000 כדי להמיר את הוראות ההדפסה לשפת המדפסת. עליך להכיר גם את הדרישות עבור הדפסה ברשת, הכוללות לפחות מחשב אחד המשמש כשרת הדפסה, מספיק זיכרון RAM ומספיק שטח פנוי בכונן הדיסק הקשיח. עליך גם לקבוע את דרישות ההדפסה של המשתמשים ושל החברה, מספר שרתי ההדפסה הנדרשים והיכן יש למקם את התקני ההדפסה. בסביבת Windows 2000 קיימים מספר שילובים אפשריים של לקוחות, שרתים והתקני הדפסה, תלוי אם התקן ההדפסה הוא מקומי או מרוחק, ואם הוא מחובר ישירות למחשב או שהוא התקן רשת.

שיעור 2: הגדרת מדפסות רשת

הגדרת מדפסת רשת ושיתופה מאפשרים למשתמשים רבים להדפיס באמצעותה. ניתן להגדיר Printer ל-Print Device המחובר ישירות לשרת ההדפסה, או להגדיר Printer עבור Print Device המחובר לשרת ההדפסה דרך הרשת. בארגונים גדולים, רוב ה-Printers מצביעות ל-Network Print Devices ברשת.

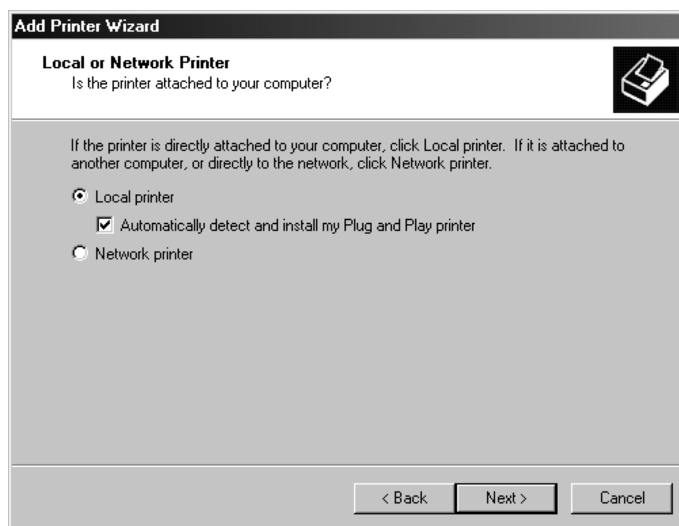
לאחר שיעור זה, תוכל

- לזהות את הדרישות להגדרת מדפסת רשת ומשאבי הדפסה ברשת.
- להוסיף ולשתף מדפסת חדשה עבור Local Print Device או עבור Network Print Device.
- לשתף Printer קיים.

זמן שיעור משוער: 35 דקות

התקנת Local Print Device

הצעדים להוספת Printer (מדפסת לוגית) עבור Local Print Device או עבור Network Print Device, דומים. כדי להתקין Local Print Device, השתמש באשף הוספת מדפסות שבשרת ההדפסה. כאשר תישאל, בחר Local Printer ולא Network Printer, כפי שמוצג בתרשים 8.6.



תרשים 8.6 מסך הבחירה בין מדפסת מקומית או מדפסת רשת מופיע באשף Add Printer.

האשף מדריך אותך בצעדים הנוספים הדרושים כדי להוסיף מדפסת עבור התקן הדפסה המחובר לשרת ההדפסה. מספר התקני ההדפסה המקומיים שניתן לחבר לשרת הדפסה באמצעות יציאות פיסיות, תלוי בתצורת החומרה של השרת, ובדרך כלל 4.

התקנת Network Print Device

בחברות גדולות, רוב התקני ההדפסה הם מדפסות רשת. להתקני הדפסה אלה יש כמה יתרונות. אין צורך למקם את התקני ההדפסה (הברזלים) קרוב לשרת ההדפסה. בנוסף, חיבורי רשת בארכיטקטורות חדשות מעבירים נתונים במהירות גבוהה יותר, מזו המתבצעת באמצעות כבלי מדפסת מקבילים.

הוספת מדפסת לוגית עבור התקן הדפסה מתבצעת באמצעות אשף Add Printer. ההבדל העיקרי בין הוספת מדפסת לוגית עבור Local Print Device, לבין הוספתה עבור Network Print Device, הוא שעבור התקן הדפסה מרוחק טיפוסי יש לספק יציאה נוספת ומידע לגבי פרוטוקול רשת.

ברירת המחדל של פרוטוקול הרשת עבור Windows 2000 הוא פרוטוקול TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol), הנמצא בשימוש רבים מהתקני ההדפסה ברשת. ניתן לספק מידע נוסף אודות היציאה על ידי שימוש באשף Add Standard TCP/IP Printer Port (הוסף פרוטוקול TCP/IP סטנדרטי ליציאת המדפסת). לפרטים נוספים על התקנת התקן הדפסה TCP/IP ברשת, ראה בעזרה של Windows 2000 Server.

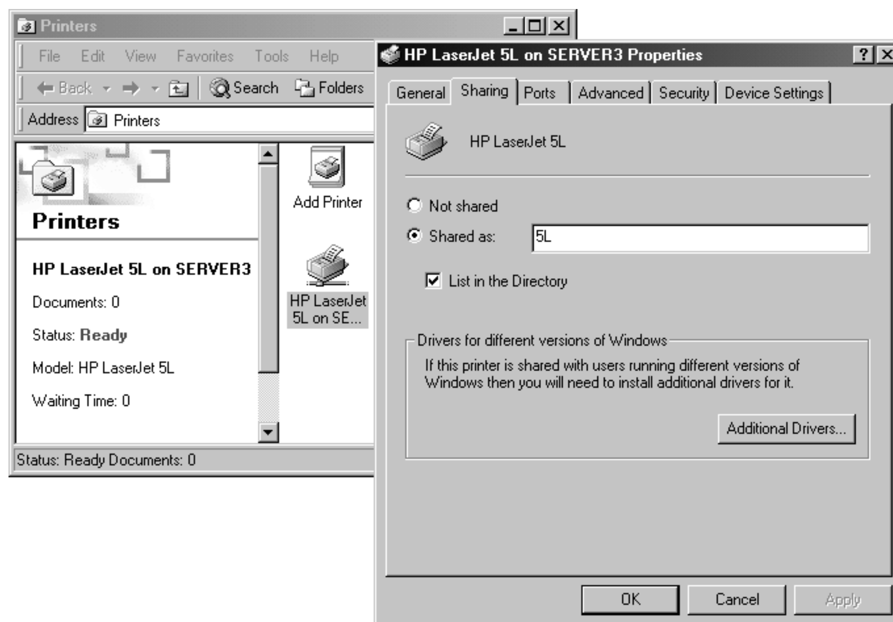
שיתוף התקן הדפסה קיים

אם דרישות ההדפסה ברשת גדלות, וברשת קיים התקן הדפסה שאינו משותף, ניתן לשתף אותו כדי שמשתמשים יוכלו להדפיס אליו.

כאשר משתפים מדפסת לוגית יש להתחשב בהנחיות הבאות:

- יש להקצות למדפסת הלוגית שם שיתוף שיופיע ב- My Network Places. יש להשתמש בשם אינטואיטיבי, כדי לסייע למשתמשים באיתור המדפסת.
- ניתן להוסיף מנהלי התקן (Printer Drivers) עבור Windows 9x, כל גרסאות Windows NT, ו- Windows 2000.
- ניתן לבחור לפרסם את המדפסת הלוגית ב-Active Directory Services, כך שמשתמשים יוכלו לבצע חיפוש אחר המדפסת.

כדי לשתף מדפסת קיימת, פתח את חלון Printers, בחר מדפסת, לחץ עליה לחיצה ימנית, מתפריט הקיצור בחר Properties ובחר בכרטיסיה Sharing (תרשים 8.7). הכרטיסיה Sharing מספקת ממשק פשוט לשיתוף מדפסת.



תרשים 8.7 הכרטיסיה Sharing שבתיבת הדו-שיח Properties של המדפסת.

אחרי שיתוף המדפסת הלוגית, תציג Windows 2000 סמל של יד כף יד מושטת מתחת לסמל המדפסת, כדי לסמן שמדפסת זו משותפת.

תרגיל 1: התקנה והגדרה של שיתוף הדפסה והגדרת מדפסת לפעולה לא מקוונת (Offline)

בתרגיל זה תשתמש באשף Add Printer (הוספת מדפסת) כדי להוסיף למחשב מדפסת מקומית ולשתף אותה. תרגיל זה אינו דורש התקן הדפסה, כיון שהמדפסת תופעל בצורה לא מקוונת, כדי למנוע את אפשרות הופעתן של הודעות שגיאה בתרגילים הבאים. סיים תרגיל זה במחשב Server01.

הליך 1: הוספת מדפסת מקומית והגדרת שיתוף הדפסה

1. התחבר לתחום (Domain) כמנהל (Administartor) עם הסיסמה password.
2. לחץ על לחצן Start, הצבע על Settings ולחץ על Printers.

   החלון Printers יופיע ובו הסמל FAX. במהלך התקנה טיפוסית של שרת Windows 2000 מותקנים בו גם שירותי FAX.
3. לחץ לחיצה כפולה על Add Printer. על המסך יופיע החלון הראשון של האשף Add Printer.

4. לחץ Next. מסך Local Or Network Printer (מדפסת רשת או מדפסת מקומית) יופיע, וניתנת הנחיה לבחירת מיקום המדפסת. כיון שאתה מתקין מדפסת במחשב המקומי ולא במחשב אחר, עליך להתייחס למדפסת שאתה מתקין כאל מדפסת מקומית.

5. ודא שלחצן האפשרויות Local Printer נבחר. נקה את תיבת הסימון שליד Automatically Detect And Install My Plug And Play Printer, ולחץ Next. מסך Select The Printer Port יופיע.

6. לחץ על לחצן האפשרויות Create A new Port. תיבת הרשימה הנפתחת Type תופיע.

7. לחץ על החץ הימני שבתיבת הרשימה הנפתחת Type. שים לב שהאפשרויות הזמינות הן Local Port ו- Standard TCP/IP Port.

   סוגי היציאה האחרים שיכולים להיות זמינים, תלויים בסוג הפרוטוקולים של הרשת המותקנים במחשב. במקרה זה מותקן פרוטוקול TCP/IP, כך שהיציאה המבוססת על פרוטוקול זה, זמינה.

8. לחץ על לחצן האפשרויות Use The Following Port, וודא ש- LPT1 מסומנת. לצורך תרגיל זה, הנח שהתקן ההדפסה שאתה מוסיף מחובר ישירות למחשב באמצעות היציאה LPT1.

9. לחץ Next. האשף ישאל אותך לגבי יצרן ודגם המדפסת. בחר להוסיף מדפסת מתוצרת HP דגם HP LaserJet 5Si.

טיפ רשימת המדפסות ממוינת בסדר אלפאביתי. אם אינך יכול למצוא את שם המדפסת, ודא שאתה מחפש במקום הנכון.

---

10. מהרשימה Manufacturers בחר HP; מהרשימה Printers בחר במדפסת HP LaserJet 5Si ולחץ Next.

    מסך Name Your Printer יופיע. המדפסת המופיעה כברירת המחדל של Windows 2000 היא HP LaserJet 5Si בתרגיל זה, אל תשנה את השם.

11. ודא שנבחר לחצן האפשרויות Do You Want Your Windows-Based Programs To Use This Printer As Default Printer?.

12. לחץ Next. מסך Printer Sharing יופיע וידרוש את נתוני השיתוף.

13. ודא שלחצן האפשרויות Share As נבחר.

שים לב שביכולתך לציין שם שיתוף למדפסת, למרות שכבר ציינת שם עבור המדפסת עצמה. שם השיתוף של המדפסת משמש לזיהוי המדפסת ברשת וחייב להתאים למוסכמות מתן השמות. שם השיתוף שונה משם המדפסת אותו בחרת קודם. שם המדפסת הוא תיאור שיופיע עם סמל המדפסת בתיקיית המערכת Printers ובשירותי Active Directory. שם השיתוף הוא קצר, כדי להבטיח תאימות למערכות הפעלה אחרות, כגון Windows 3.x.

14. בתיבת הטקסט Share As, הקלד **Printer1** ולחץ Next.

מסך Location And Comment יופיע.

הערה Windows 2000 מציגה את הערכים שהכנסת לתיבות הטקסט Location ו-Comment, כשמשתמש סורק את ה- Active Directory כדי לאתר מדפסת. הוספת נתונים בתיבות אלו אינה חובה, אך נתונים אלה יסייעו למשתמש לאתר מדפסת.

---

15. בתיבת הטקסט Location הקלד **building 520 / floor 18 /office 1831**, בתיבת הטקסט Comment הקלד **מדפסת לייזר שחור-לבן - להדפסות ארוכות**; ולחץ Next.

מסך Print Test Page (הדפס דף בדיקה) יופיע. ניתן להדפיס דף בדיקה כדי לוודא שהמדפסת מכוונת כראוי. כמו כן, ניתן להתקין Printer Drivers אחרים עבור גרסאות אחרות של Windows.

16. לחץ על לחצן האפשרויות No, ולחץ Next.

המסך Completing The Add Printer Wizard יופיע ויציג את סיכום הגדרות ההתקנה שבחרת.

17. אשר את סיכום הגדרות ההתקנה, ולחץ Finish.

אם נדרש, Windows 2000 תציג את תיבת הדו-שיח Files Needed ובה תתבקש לספק את הנתיב לקבצי ההתקנה המקוריים של Windows 2000 Server.

18. אם תיבת הדו-שיח Files Needed מופיעה, הכנס את תקליטור ההתקנה של Windows 2000 Server והמתן כ-10 שניות. אם תיבת הדו-שיח Files Needed אינה מופיעה דלג ישר לסעיף 20.

19. אם מופיע החלון Windows 2000 CD-ROM, סגור אותו.

20. לחץ OK כדי לסגור את תיבת הדו-שיח Insert Disk. Windows 2000 תעתיק את קבצי המדפסת ובחלון Printers יופיע סמל עבור המדפסת HP LaserJet 5Si.

שים לב ש- Windows 2000 מציגה מתחת לסמל המדפסת סמל יד מושטת. זהו הסימן לכך שזהו שיתוף רשת. שים לב גם לסימן ה- ✓ שליד סמל המדפסת, סימן זה מציין כי מדפסת זו היא מדפסת ברירת המחדל עבור שרת ההדפסה.

21. השאר את חלון Printers פתוח, מכיון שנזדקק לו להשלמת התרגיל הבא.

הליך 2: העברת מדפסת למצב לא מקוון והדפסת מסמך לניסיון

בתרגיל זה תעביר את המדפסת שיצרת למצב לא מקוון (Offline). העברת מדפסת למצב לא מקוון גורמת למסמכים הנשלחים אליה להישאר במחשב, כל עוד המדפסת אינה זמינה. פעולה זו תמנע הופעתן של הודעות שגיאה אודות התקני הדפסה לא זמינים בהליכים הבאים. אחרת, Windows 2000 תציג הודעות שגיאה כאלו כשהיא מנסה לשלוח מסמך להדפסה בהתקן שאינו מחובר למחשב.

1. בחלון Printers לחץ על סמל HP LaserJet 5Si.
2. פתח את תפריט File ובחר באפשרות Use Printer Offline.

   שים לב לכך ש- Windows 2000 משנה את סמל המדפסת, כדי לציין שמדפסת זו אינה זמינה והטקסט בחלונית השמאלית של חלון Printers מציין שמצב המדפסת הוא Use Printer Offline.
3. בחלון Printers לחץ לחיצה כפולה על סמל המדפסת HP LaserJet 5Si. שים לב שרשימת המסמכים שנשלחו להדפסה ריקה.
4. לחץ על Start, הצבע על Programs, הצבע על Accessories ולחץ על Notepad.
5. בחלון Notepad הקלד טקסט כלשהו, כרצונך.
6. ארגן את חלונות Notepad והמדפסת כך שתוכל לראות את התוכן של שניהם.

טיפ לחץ לחיצה ימנית על מקום ריק בשורת המשימות ומתפריט הקיצור בחר באפשרות Tile Windows Horizontally.

---

7. בחלון Notepad פתח את תפריט File ובחר Print. תיבת הדו-שיח Print תופיע ותאפשר בחירת מדפסת ואפשרויות הדפסה.

   תיבת הדו-שיח Print מציגה את הערת המיקום והתיאור שהוספת למדפסת, וגם מודיעה לך במידה והמדפסת אינה מקוונת. תוכל להיעזר גם בלחצן Find Printer שבתיבת הדו-שיח, כדי לחפש את המדפסת במחסן Active Directory.

   שים לב שהמדפסת הנבחרת היא HP LaserJet 5Si. מדפסת זו נבחרת באופן אוטומטי, כיון שהיא זו המוגדרת כברירת המחדל בשרת ההדפסה.
8. לחץ Print. Notepad תציג להרף עין הודעה המציינת כי המסמך מודפס. במחשב מהיר ייתכן אף שלא תזכה לראות את ההודעה הזו.

   בחלון HP LaserJet 5Si - Use Printer Offline תראה את המסמך ממתין להישלח להתקן ההדפסה. המסמך מוחזק בתור ההדפסה כיון שהעברת את המדפסת למצב לא-מקוון. אם המדפסת היתה מקוונת, היה המסמך נשלח להתקן ההדפסה.

9. סגור את חלון Notepad וכאשר תישאל האם לשמור את השינויים שערכת במסמך לחץ No.

10. בחלון HP LaserJet 5Si - Use Printer Offline בחר במסמך הממתין, פתח את תפריט Printer ולחץ Cancel All Documents.

    תיבת הודעה Printers תופיע ובה תישאל האם אתה בטוח שברצונך לבטל את כל המסמכים הממתינים להדפסה בהתקן ההדפסה הנבחר HP LaserJet 5Si.

11. לחץ Yes. המסמך יוסר מתור ההדפסה.

12. סגור את החלון HP LaserJet 5Si - Use Printer Offline.

13. סגור את החלון Printers.

סיכום שיעור

הצעדים להוספת מדפסת מקומית או מדפסת רשת הם דומים. בשני המקרים השתמש באשף Add Printer בשרת ההדפסה. אשף Add Printer מתחיל בחלון Welcome To The Add Printer Wizard. האשף מדריך אותך דרך הצעדים הדרושים להוספת מדפסת לוגית להתקן הדפסה. פרוטוקול ברירת המחדל עבור רשת Windows 2000 הוא TCP/IP, בו משתמשות מדפסות רשת רבות. בנוסף, אם דרישות עבודות ההדפסה ברשת שלך גדלות, וברשת קיים התקן הדפסה שאינו משותף, תוכל ליצור שיתוף עבור התקן זה ולאפשר למשתמשים אחרים להדפיס באמצעותו.

שיעור 3: ניהול מדפסות רשת

בחלק זה תלמד אודות הגדרה וניהול מדפסות רשת. השיעור דן בניהול מדפסות ומסמכים, בשימוש בדפדפן אינטרנט לניהול מדפסות, בהגדרת קבוצת מדפסות (Printer pool), בהגדרת קדימויות בין מדפסות ובאיתור וטיפול בתקלות הדפסה שכיחות.

לאחר שיעור זה, תוכל

- לגשת למדפסות ולהגדיר הרשאות.
- לנהל מדפסות ומסמכים.
- להשתמש בדפדפן אינטרנט כדי לנהל מדפסות.
- להגדיר קבוצת מדפסות.
- להגדיר קדימויות בין מדפסות.

זמן שיעור משוער: 90 דקות

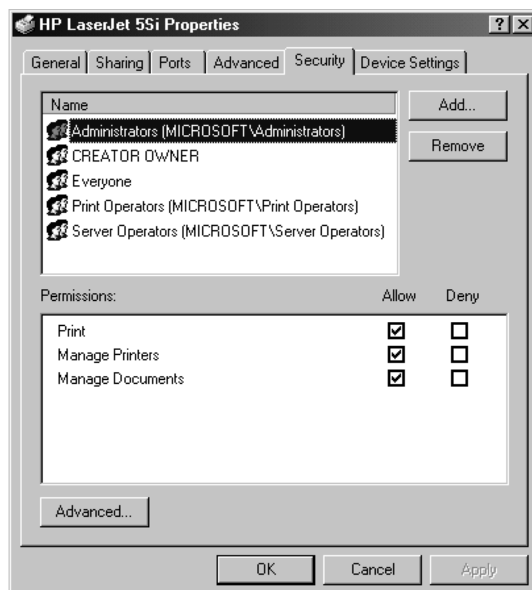
גישה למדפסות

תוכל לקבל גישה למדפסות לצרכי ניהול באחת משתי הדרכים הבאות:

- ❖ מחלון Printers שבתפריט Start, Settings.
- ❖ לחצן Find שבתוסף התוכנה Active Directory Users And Computers (Snap-in), או לחצן search בתפריט start ולבחור בחיפוש ... For Printers.

חלון Printers מאפשר לך לבצע את כל משימות הניהול; לעומת זאת, חלק ממשימות הניהול אינו ניתן לביצוע מתוך חלון חיפוש. לדוגמה, אינך יכול להשתמש בחלון חיפוש כדי לבצע העברת מדפסת למצב לא-מקוון. כדי להעברת מדפסת למצב לא-מקוון, עליך לגשת למדפסת המבוקשת מחלון Printers.

Windows 2000 מאפשרת לך לשלוט בשימוש ובניהול המדפסת על ידי הגדרת הרשאות בכרטיסיה Security שבתיבת הדו-שיח Properties של המדפסת (תרשים 8.8). השימוש בהרשאות עבור המדפסת מאפשר לך לקבוע איזה משתמשים יכולים להשתמש במדפסת זו. תוכל גם לקבוע הרשאות למדפסת, כדי לקבוע מי יכול לנהל את המדפסת, ואת רמת הרשאת הניהול שתינתן לו, שיכולה לכלול ניהול מדפסת וניהול מסמכים.



תרשים 8.8 הרשאות ברירת המחדל המוגדרות למדפסת, כפי שמופיעות בכרטיסיה Security שבתיבת הדו-שיח Properties של המדפסת HP LaserJet 5Si.

מטעמי אבטחה, ייתכן שתצטרך להגביל גישת משתמשים למדפסות מסוימות. תוכל גם להשתמש בהרשאות עבור המדפסות כדי להאציל אחריות על מדפסות מסוימות למשתמשים שאינם administartors. Windows 2000 מאפשרת שלוש רמות של הרשאות מדפסת:

- Print (הדפסה),
- Manage Printers (ניהול מדפסות),
- Manage Documents (ניהול מסמכים),

כפי שניתן לראות בתיבה Permissions בתרשים 8.8.

הרשאות מדפסת ניתן לאפשר (Allow) או למנוע (Deny). כמו במדיניות קבוצה והרשאות NTFS, הרשאות מסוג Deny תמיד "ידרסו" הרשאות Allow (הן חזקות יותר). לדוגמה, אם תבחר את קבוצת המערכת Everyone המופיעה בתרשים 8.8 ותסמן את תיבת הסימון Deny בשורה Manage Documents, אף אחד ברשת כולל Administrator לא יוכל לנהל מסמכים, אפילו אם הגדרת הרשאה המאפשרת זאת לחשבון משתמש אחר, או קבוצה. זאת מכיון שכל חשבונות המשתמשים חברים בקבוצת המערכת Everyone.

כברירת מחדל, Windows 2000 מקצה את כל הרשאות ההדפסה לקבוצת המערכת Everyone, ובכך מאפשרת לכל המשתמשים לשלוח הדפסה למדפסת זו. ניתן גם להגדיר הרשאות לגבי המדפסת עבור משתמשים או קבוצות. תוכל לשנות את הרשאות ברירת המחדל שהוגדרו על ידי Windows 2000, או את אלו שהגדרת אתה בעבר, לגבי כל קבוצה או משתמש.

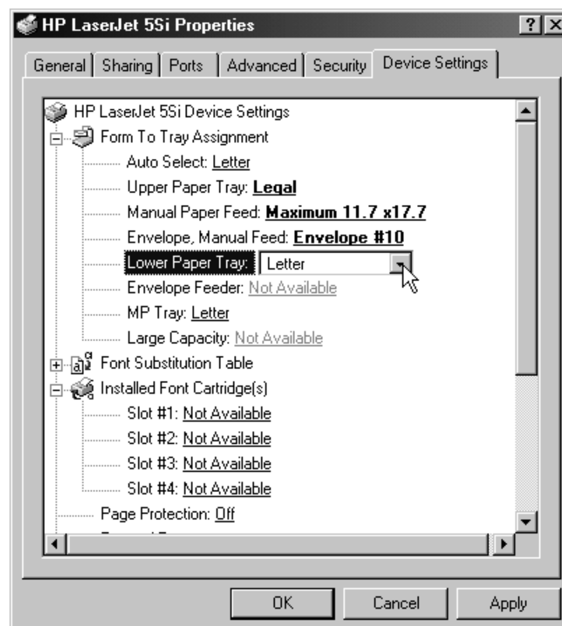
ניהול מדפסות

ניהול מדפסות כולל שיוך גדלי נייר שונים למגשי ההזנה והגדרת דפים מפרידים (Separator page). בנוסף, אם מתרחשת תקלה ב-Print Device (התקן הדפסה) תוכל להשהות, להפעיל מחדש או לבטל את כל עבודות ההדפסה שבתור ההדפסה (או מסמך יחיד). אם אירעה תקלה בהתקן הדפסה, או שהוספת התקני הדפסה נוספים לרשת שלך, ייתכן שתצטרך להפנות את המסמכים למדפסת שונה. תצטרך גם לקבוע מחדש למי יש אחריות ניהולית בלתי מוגבלת למדפסת, דבר הדורש שינוי בעלות על מדפסת.

שיוך נייר בגדלים שונים למגשי הזנה

אם ל-Printer Device (התקן הדפסה) יש מספר מגשי הזנה, בהם מוזנים בדרך כלל סוגי נייר בגדלים שונים, תוכל לשייך את גדלי הנייר למגשים מסוימים. במקרים מסוימים תמצא התייחסות למונח **Form** (טופס) - הכוונה היא לגודל הנייר (Paper size). המשתמשים יוכלו לבחור את גודל הנייר הרצוי להם מתוך היישום בו הם עובדים. כאשר המשתמש מדפיס מסמך, Windows 2000 מנתבת באופן אוטומטי את עבודת ההדפסה לאותו מגש בו מוזן נייר בגודל הרצוי. דוגמאות לגדלי נייר (טפסים) הן : Legal, Letter, A4 ו- Executive.

כדי לשייך גודל נייר למגש הזנה, פתח את חלון Printers, לחץ לחיצה ימנית על המדפסת המבוקשת ומתפריט הקיצור בחר Properties. בתיבת הדו-שיח Properties של המדפסת בחר בכרטיסיה Device Settings, כמוצג בתרשים 8.9. כאן תוכל להגדיר את גדלי הנייר הנדרשים.



תרשים 8.9 הכרטיסיה Device Settings עבור המדפסת HP LaserJet 5Si.

לאחר שהגדרת את מגש הנייר, מציין המשתמש את גודל הנייר מתוך היישום בו הוא עובד. Windows 2000 יודעת איזה גודל נייר נמצא באיזה מגש הזנה.

שים לב שבתרשים 8.9 מופיעות מספר אפשרויות בגוון דהוי. אפשרויות אלו אינן מותקנות, או שאינן זמינות במדפסת האמורה. המאפיינים המופיעים בכרטיסיה Device Settings נקבעים על ידי מנהל ההתקן (Driver) של התקן ההדפסה. לדוגמה, למדפסת לייזר אישית מסוג HP LaserJet 5L יש רק שתי אפשרויות הזנת נייר: מזין הנייר האוטומטי (נקרא Paper Input Bin) ומגש הזנת נייר ידני. שים לב שבתרשים 8.9 מציגה הכרטיסיה Device Settings שבע אפשרויות הזנת נייר ומאפיינים רבים נוספים, אשר אינם זמינים בכל התקן הדפסה אחר.

הגדרת דף מפריד

דף מפריד (Separator Page) הוא קובץ המכיל פקודות התקן הדפסה. דפים מפרידים משמשים לשתי מטרות:

- לזיהוי ולהפרדה בין מסמכים מודפסים.
- למעבר בין מצבי הדפסה שונים. התקני הדפסה אחדים יכולים לעבור בין מצבי הדפסה שונים, המנצלים מאפיינים שונים של התקן ההדפסה. תוכל להיעזר בדף המפריד כדי לציין את שפת ההדפסה המתאימה. לדוגמה, אם התקן ההדפסה שלך תומך במעבר בין שפות הדפסה שונות, אך אינו יודע לזהות באופן אוטומטי את שפת עבודת ההדפסה, תוכל לציין להתקן ההדפסה לפעול בשפת PostScript או בשפת PCL - **P**rinter **C**ontrol **L**anguage.

Windows 2000 כוללת ארבעה קבצי דף מפריד. תמצא אותם בתיקיה %systemroot%\System32. הטבלה הבאה מציגה את שם הקובץ ומתארת את הפעולה שהוא מבצע:

שם הקובץ	פעולה
Pcl.sep	מעביר את מצב ההדפסה למצב PCL עבור התקני הדפסה HP ומדפיס דף מפריד לפני כל עבודת הדפסה.
Pscript.sep	מעביר את מצב ההדפסה למצב PostScript עבור התקני הדפסה HP, אך אינו מדפיס דף מפריד לפני כל עבודת הדפסה.
Sysprint.sep	מדפיס דף מפריד לפני כל עבודת הדפסה. תואם להתקני הדפסה מסוג PostScript.
Sysprtj.sep	גירסה של הקובץ Sysprint.sep המשתמשת בערכת תווים יפנית.

תוכל ליצור דפים מפרידים מותאמים אישית על ידי יצירת דפי sep, המכילים פקודות מדפסת חוקיות. לחילופין, תוכל להתאים את קבצי sep הקיימים לשימושך האישי, כך שיענו על צרכיך. בחן את התיעוד המגיע עם התקן ההדפסה שלך ואתר בו את הפקודות החוקיות להתקן מסוים זה.

לאחר שהחלטת להשתמש בדף מפריד ובחרת בזה המתאים לך, בחר בכרטיסיה Advanced שבתיבת הדו-שיח Properties של המדפסת, ולחץ על Separator Page. מתיבת הדו-שיח Separator Page תוכל להקליד את שם קובץ הדף המפריד, או להיעזר בלחצן Browse. לאחר שהדף המפריד מוגדר, הוא יודפס לפני כל עבודת הדפסה (אלא אם כן בחרת בהפרדת Pscript.sep).

השהייה, המשך וביטול מסמכים

פעולות כגון השהייה והמשך פעולת הדפסה, או ביטול כל עבודות ההדפסה במדפסת, עשויות להיות נדרשות אם מתרחשת תקלה כלשהי.

בחלון Printer קיימים שני מקומות מהם ניתן לבצע פעולות אלו. ראשית, בחר בסמל המדפסת של התקן ההדפסה לגביו אתה מעוניין לפעול ואז פתח את תפריט File. מכאן תוכל לבחור באחת מהאפשרויות, Pause Printing (השהה הדפסה) או Cancel All Documents (בטל את הדפסת כל המסמכים), או לבחור באפשרות Open מתפריט File ולבחור בפקודה המתאימה.

הטבלה הבאה מתארת את המשימות שתוכל לבצע כשאתה מנהל מדפסות, כיצד לבצע את אותן משימות וכן דוגמאות למצבים אפשריים בהם תידרש לבצע אותן.

משימה	פעולה	דוגמה
להשהיית הדפסה	לחץ על Pause Printing. סימן ✓ יופיע ליד האפשרות Pause Printing, לציין כי המדפסת מושהיית.	השהה את תהליך ההדפסה אם התרחשה תקלה במדפסת או בהתקן ההדפסה, עד שתטפל בתקלה.
להמשך ההדפסה	לחץ על Pause Printing פעם נוספת. הסימן ✓ שהופיע ליד האפשרות Pause Printing נעלם, מה שמציין כי המדפסת פעילה.	המשך את ביצוע פעולות ההדפסה לאחר שטיפלת בבעיה במדפסת או בהתקן ההדפסה.
לביטול כל המסמכים הממתינים בתור ההדפסה	לחץ על Cancel All Documents. כל המסמכים נמחקים מתור ההדפסה.	בטל את כל המסמכים כדי לנקות את תור ההדפסה, לאחר שנצברו בו מספר רב של מסמכים ישנים שכבר אין צורך להדפיסם.

הערה ניתן להשהות את פעולת ההדפסה גם על ידי העברת המדפסת למצב לא מקוון. כשאתה מעביר מדפסת למצב לא מקוון, נשארים המסמכים בתור ההדפסה אפילו אם פעולת שרת ההדפסה נפסקת (השרת "יורד") ומחודשת. כדי להעביר מדפסת למצב לא מקוון, פתח את חלון המדפסת המבוקשת, ומתפריט Printer בחר באפשרות Use Printer Offline.

ניתוב מסמכים (Redirect) למדפסת שונה

תוכל לנתב מסמכים למדפסת אחרת. לדוגמה, אם מדפסת מחוברת להתקן הדפסה לא תקין, נתב את המסמכים כך שהמשתמשים לא יצטרכו לשלוח את עבודות ההדפסה שלהם מחדש. תוכל לנתב את כל עבודות ההדפסה מהמדפסת, אך אין אפשרות לנתב מסמך מסוים. המדפסת אליה אתה מנתב את המסמכים חייבת לפעול באמצעות אותו מנהל התקן מדפסת (Printer Driver), בדיוק כמו המדפסת הלא תקינה.

לניתוב מסמכים פתח את תיבת הדו-שיח Properties של המדפסת הלא תקינה, בחר בכרטיסיה Ports והוסף יציאה (Port) נוספת.

אם התקן הדפסה (Print Device) אחר זמין לשרת ההדפסה הנוכחי, תוכל להמשיך ולהשתמש באותה המדפסת (הלוגית), ולהגדיר אותה כך שתשתמש בהתקן ההדפסה האחר. כדי להגדיר את המדפסת להשתמש בהתקן הדפסה אחר, מקומי או ברשת, אשר משתמש באותו מנהל התקן (Print Driver) בדיוק, בחר את היציאה המתאימה בשרת ההדפסה ובטל את הבחירה ביציאה הנוכחית. שים לב, מסמכים המועבדים באותו רגע בו אתה מבצע פעולה זו, אינם ניתנים לניתוב להתקן הדפסה שונה.

בעלות על מדפסת

כברירת מחדל, משתמש המתקין מדפסת - מקבל זכויות בעלות. אם משתמש זה כבר אינו יכול לנהל את המדפסת, לדוגמה, אם המשתמש שהתקין את המדפסת עוזב את הארגון - משתמש אחר צריך לקחת בעלות על המדפסת כדי לנהל אותה.

המשתמשים הבאים יכולים לקחת בעלות על מדפסת:

- ❖ משתמש או חבר בקבוצה אשר לו, או לקבוצה, יש הרשאות Manage Printers (ניהול מדפסת) עבור המדפסת המדוברת.
- ❖ חברים בקבוצות המשתמשים הבאות: Administrators, Print Operators, Server Operators, ו- Power Users. לקבוצות אלו יש הרשאות Manage Printers (ניהול מדפסת) כברירת מחדל, המאפשרות להם לקחת בעלות על מדפסת.

לקיחת בעלות על מדפסת היא תכונה מתקדמת באבטחת המערכת אשר ניתן להגיע אליה באמצעות לחצן Advanced בכרטיסיה Security שבחלון Properties של המדפסת. בעלות על מדפסת אינה יכולה להיות מוקצית על ידי משתמש אחד למשתמש אחר. אולם, Administrator יכול תמיד לקחת בעלות עבור קבוצת Administrators.

ניתן לבצע ביקורת (Auditing) כדי לאתר מי מנסה (מצליח או נכשל) לקחת בעלות על מדפסת מסוימת. גם ביצוע ביקורת, כמו לקיחת בעלות, היא תכונה מתקדמת באבטחת המערכת אשר אליה ניתן להגיע באמצעות לחצן Advanced בכרטיסיה Security שבחלון Properties של המדפסת.

ניהול מסמכים

בנוסף לניהול מדפסות, מאפשרת לך Windows 2000 לנהל גם מסמכים. ניהול מסמכים כולל השהייה, המשך, התחלה מחדש וביטול הדפסת מסמך אם אירעה תקלה. בנוסף, תוכל להגדיר למי תישלח הודעה כאשר עבודת הדפסה מסתיימת, את רמת הקדימות (אשר מאפשרת למסמכים חשובים להיות מודפסים לפני מסמכים אחרים) ולקבוע את השעה בה יודפס המסמך.

השהייה, התחלה מחדש וביטול מסמך

אם מתרחשת תקלה מסוימת בהדפסתו של מסמך, תוכל להשהות את ההדפסה ולאחר מכן להמשיך אותה. מעבר לכך, תוכל גם להתחיל את הדפסתו של מסמך מתחילתו, או לבטל את עבודת ההדפסה שלו כלל ועיקר. כדי לבצע פעולות כגון אלו, עליך להיות בעל הרשאת Manage Documents עבור המדפסת. מכיון שליוצר מסמך קיימות הרשאות ניהול למסמך שלו כברירת מחדל, יכולים משתמשים לבצע פעולות כאלו על מסמכים שלהם.

כדי לנהל מסמך, פתח את חלון המדפסת ובחר במסמך המבוקש. פתח את תפריט Document ובחר בפקודה המתאימה להשהיית הדפסת המסמך, להמשך ההדפסה, להתחלה מחדש של הדפסת המסמך הנבחר או לביטולו.

הטבלה הבאה מתארת את המשימות אותן ייתכן שתידרש לבצע בעת ניהול מסמכים יחידים, כיצד לבצע אותן ודוגמאות למצבים בהם תיאלץ לעשות זאת.

משימה	פעולה	דוגמה
להשהיית הדפסת מסמך	בחר במסמך שאת הדפסתו אתה מעוניין להשהות, ולחץ על Pause (מצב המסמך משתנה ל- Paused).	השהה את תהליך ההדפסה אם מתרחשת בעיה במסמך.
להמשך הדפסת המסמך	בחר במסמך מושהה שאתה מעוניין להמשיך את הדפסתו, ולחץ על Resume (מצב המסמך משתנה ל- Printing).	המשך את ההדפסה לאחר שטיפלת בבעיה במסמך המושהה.
להתחלת עבודת ההדפסה מתחילתה	בחר במסמך שאתה מעוניין להתחיל את הדפסתו מחדש ולחץ על Restart. כך מתחילה הדפסת המסמך מראשיתו.	התחל את ההדפסה מחדש במקרה של מסמך שהודפס בחלקו, לאחר שתיקנת בעיה במסמך או בהתקן ההדפסה.
לביטול הדפסת המסמך	בחר במסמך שאת הדפסתו אתה מעוניין לבטל, ולחץ Cancel. ניתן לבטל הדפסת מסמך גם על ידי הקשה על מקש Del.	כאשר למסמך מוגדרות הגדרות מדפסת שגויות, או שהוא כבר אינו נדרש, מחק אותו לפני שיודפס.

הגדרת הודעות, קדימויות וזמני הדפסה

ניתן לשלוט בעבודות הדפסה על ידי הגדרת הודעות (Notify), קדימויות (Priority) וזמני הדפסה (Schedule). כדי לבצע את משימות ניהול המסמכים הללו עליך להיות בעל הרשאת Manage Documents (ניהול מסמכים) במדפסת האמורה.

את הגדרת ההודעות, הקדימויות וזמני ההדפסה מבצעים בכרטיסיה General של תיבת הדו-שיח Properties של המסמך. כדי לפתוח את תיבת מאפייני המסמך פתח את חלון המדפסת מתוך התיקיה Printers, בחר את המסמך המבוקש פתח את תפריט Documents ובחר Properties.

הטבלה הבאה מתארת את המשימות אותן ייתכן שתידרש לבצע בעת ניהול עבודות הדפסה, כיצד לבצע אותן ודוגמאות למצבים בהם תיאלץ לעשות זאת.

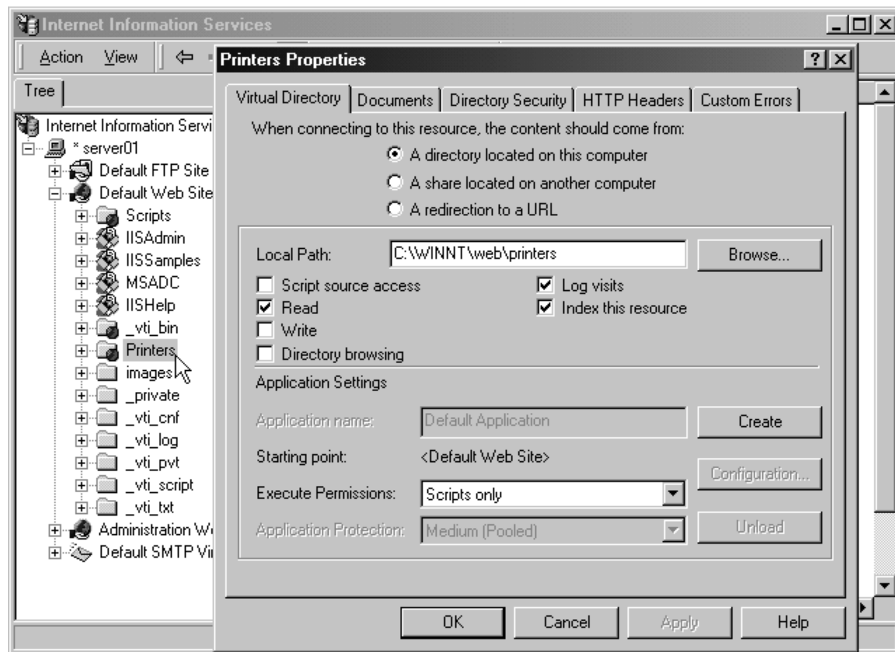
משימה	פעולה	דוגמה
הגדרת הודעה	בתיבת הדו-שיח Notify הקלד את שם המשתמש שאמור לקבל את ההודעות. כברירת מחדל מכניסה Windows 2000 את שם המשתמש שהדפיס את המסמך.	שנה את הודעת ההדפסה כאשר מישהו אחר, לא זה ששלח את ההדפסה, אמור לקבל את הפלט המודפס.
שינוי קדימות מסמך	הזז את גררת הקדימות (Priority) לרמת הקדימות הרצויה לך. הקדימות הגבוהה ביותר היא 99 והנמוכה ביותר היא 1.	שנה את קדימות המסמך כדי שמסמכים חשובים יודפסו לפני מסמכים אחרים.
תזמון מועדי הדפסה	כדי להגביל את מועדי ההדפסה לחץ על Only From בתיבה Schedule, והגדר את השעות שבהן אתה מעוניין להדפיס את המסמך.	הגדר את מועד ההדפסה של מסמך גדול כך שידפיס בשעות בהן אין פעילות במשרד, כגון בשעות הלילה המאוחרות. במצב זה, ניתן לשלוח הדפסות למדפסת במשך כל היום, אלא שהן תודפסנה רק בזמנים שהוגדרו להן.

ניהול מדפסות באמצעות דפדפן אינטרנט

Windows 2000 מאפשרת לך לנהל מדפסות מכל מחשב בו פועל דפדפן אינטרנט, בין אם המחשב פועל בסביבת Windows 2000, או אם מותקן בו Printer Driver (מנהל התקן המדפסת) המתאים. באמצעות כמעט כל אחד מדפדפני האינטרנט השכיחים, וללא קשר ותלות במערכת ההפעלה של המחשב, יכולים משתמשים לצפות בדפי אינטרנט המציגים את מצב שרת ההדפסה של Windows 2000 והמדפסות המותקנות בו. כל משימות הניהול אותן אתה מבצע באמצעות כלי הניהול של Windows 2000

מתבצעות באותו אופן כאשר אתה מבצע אותן באמצעות דפדפן אינטרנט. ההבדל בניהול באמצעות דפדפן אינטרנט הוא בממשק, שהוא ממשק מבוסס HTML. כדי ששרת Windows 2000 המשמש כשרת הדפסה יתמוך בהצגת דפי אינטרנט יש להתקין בו IIS - **S**ervices **I**nformation **I**nternet Microsoft. כדי ששרת הדפסה מבוסס Windows 2000 Professional יתמוך בהצגת דפי אינטרנט יש להתקין ולהגדיר בו את Microsoft **P**er **W**eb **S**erver - PWS.

כאשר IIS מותקן, נוצרת תיקיה וירטואלית בשם Printers, מתחת ל- Default Web Site, כפי שניתן לראות בתרשים 8.10. תיקיה וירטואלית זו היא מצביע לתיקיה %systemroot%\web\printers.



תרשים 8.10 הכרטיסיה Virtual Directory שבתיבת הדו-שיח Printers Properties.

השימוש בדפדפן אינטרנט לניהול מדפסות

לשימוש בדפדפן אינטרנט לניהול מדפסות יש מספר יתרונות:

- הוא מאפשר ניהול מדפסות מכל מחשב בו פועל דפדפן אינטרנט, בין אם מערכת ההפעלה בו היא Windows 2000 ובין אם לא, וללא תלות בהתקנת Printer Driver (מנהל התקן המדפסת) המתאים.
- הוא מאפשר יצירת ממשק מותאם אישית. לדוגמה, אתה יכול ליצור את דף האינטרנט שלך המכיל את תרשים הקומה ובו מיקומי המדפסות והקישורים אליהן.

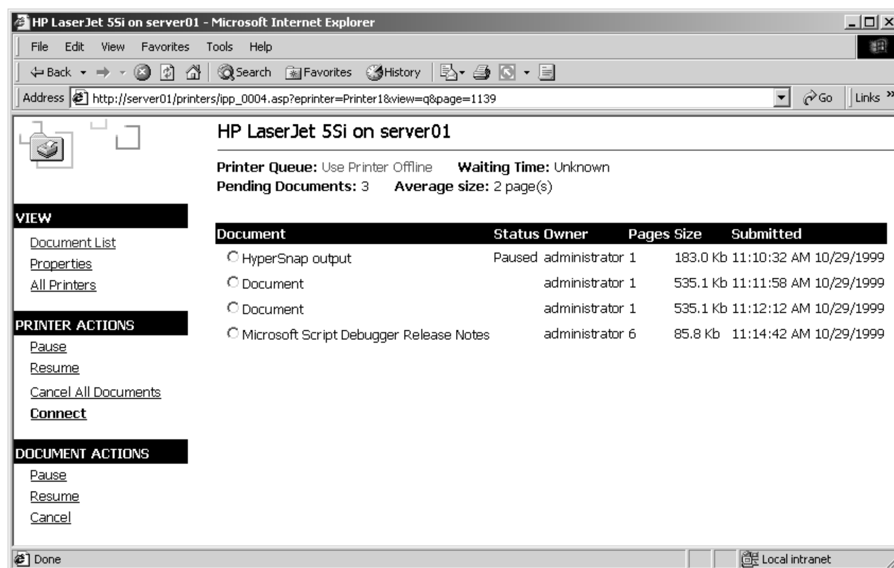
❖ הוא מפיק דף מסכם, המציין את מצבן של כל המדפסות בשרת ההדפסה.

❖ הוא יכול לדווח בזמן אמת את נתוני המדפסת, כגון האם התקן ההדפסה עבר למצב חיסכון באנרגיה, אם מנהל התקן המדפסת מאפשר הפקת מידע כגון זה. מידע זה אינו זמין בחלון Printers.

גישה למדפסות באמצעות דפדפן אינטרנט

אם אתה מעוניין לבצע גישה לשרת ההדפסה תוך שימוש בדפדפן אינטרנט הפעל את דפדפן האינטרנט והפנה אותו לכתובת הבאה: http://<print_server>/printers.

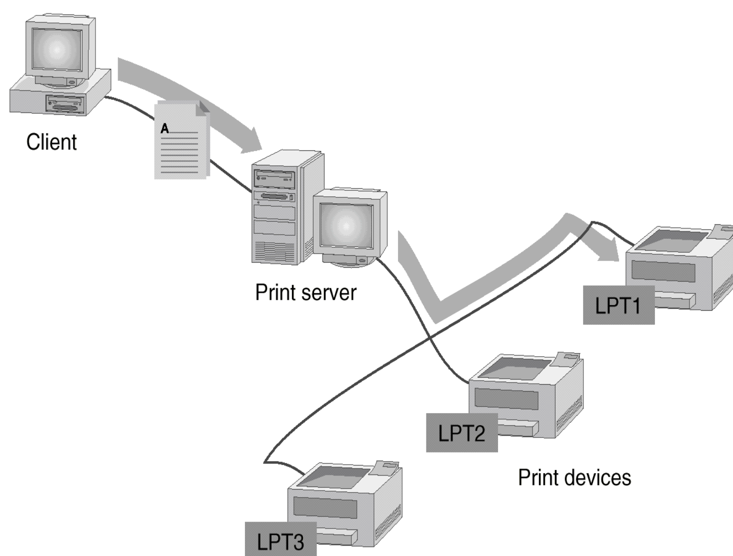
אם אתה מעוניין לבצע גישה למדפסת מסוימת מבלי לצפות תחילה ברשימת כל המדפסות, הקלד את הכתובת **http://<print_server>/<share>**. תרשים 8.11 מציג כיצד ייראה דף האינטרנט כאשר תבצע גישה לשיתוף Printer1 שבשרת Server01. שים לב שלאחר שתקליד את הכתובת **http://Server01/printer1** מנותבת הכתובת המופיעה בשורה Address, באמצעות דפי שרת פעילים (**A**ctive **S**erver **P**ages - ASP), לכתובת http://server01/printers/ipp_0004.asp?eprinter=Printer1&view=q&page=1139.



תרשים 8.11 דף האינטרנט המציג את המדפסת HP LaserJet 5Si בשרת Server01.

הגדרת Printer Pool

Printer Pool היא Printer (מדפסת לוגית) אחת המחוברת למספר התקני הדפסה (Print Devices) באמצעות מספר יציאות בשרת ההדפסה. התקני ההדפסה יכולים להיות מקומיים או התקני הדפסה ברשת. מומלץ שהתקני המדפסת יהיו זהים; אולם, תוכל להשתמש ב-Print Devices שאינם זהים אך להשתמש באותו Printer Driver עבור כולם. תרשים 8.12 מציג Printer Pool הכוללת שלושה Print Devices.



תרשים 8.12 הדפסה ל-Printer Pool הכוללת שלושה Print Devices.

לפי תרשים 8.12, היצירה של Printer Pool גרמה לכך שהמשתמש "רואה" רק מדפסת לוגית אחת, בעוד שרת ההדפסה "רואה" שלושה התקני הדפסה לפניו, אליהם הוא יכול לשלוח את ההדפסה למדפסת הפנוייה ובכך להקטין את זמן ההמתנה להדפסה. כשאתה יוצר Printer Pool, משתמשים יכולים לשלוח הדפסות, מבלי לחפש איזה התקן הדפסה זמין - ה-Printer (המדפסת הלוגית) בוחנת איזו יציאה פנויה. קיבוץ מדפסות מוגדר בכרטיסיה Ports שבתיבת הדו-שיח Properties של המדפסת. פתח את תיבת הדו-שיח, עבור לכרטיסיית Ports וסמן את תיבת הסימון Enable Printer Pooling שבתחתית הכרטיסיה. אחר כך צור או בחר את היציאות המכילות את אותם התקני הדפסה שיהוו חלק מה-Printer Pool שאתה יוצר.

הערה כשאתה **יוצר** Printer Pool (קבוצת מדפסות), הצב את התקני ההדפסה (Print Devices, מדפסות פיסיות) באותו מיקום פיסי, כדי שהמשתמשים **יוכלו** לאתר את עבודות ההדפסה שלהם בקלות. אם לא תציב את התקני ההדפסה במיקום פיסי קרוב יגרום הדבר לכך שמשתמשים לא ידעו לאיזו מדפסת נשלחה עבודת ההדפסה שלהם (הצד החיובי הוא שהם יזכו לתרגול נוסף בניסיון לחפש אחר המסמכים שלהם...).

ל-Printer Pool יש את היתרונות הבאים:

- ❖ בסביבת רשת בה כמות ההדפסות גדולה יקטין שימוש במאגר מדפסות את הזמן בו ממתינים מסמכים בתור בשרת ההדפסה.
- ❖ הדבר מפשט את ניהול הרשת, מכיון שאתה יכול לנהל מספר התקני הדפסה באמצעות מדפסת לוגית אחת!

לפני שתיצור Printer Pool, ודא שהתקני ההדפסה מחוברים כראוי לשרת ההדפסה או לרשת.

הגדרת עדיפויות (Priorities)

Priority setting בין מדפסות מאפשרת הגדרת עדיפויות בין קבוצות מסמכים, שכולם מודפסים לאותו התקן הדפסה (Print Device). מספר מדפסות לוגיות (Printers), אשר כולן מצביעות לאותו התקן הדפסה מאפשר למשתמשים לשלוח מסמכים חשובים ל-Printer לה מוגדרת עדיפות גבוהה, ומסמכים פחות חשובים ל-Printer בעדיפות נמוכה יותר. המסמכים החשובים תמיד יודפסו ראשונים. כדי להגדיר עדיפויות בין מדפסות, הגדר שתי Printers (מדפסות לוגיות) לפחות שיצביעו לאותו Print Device (התקן הדפסה) - זאת אומרת, לאותה יציאה (Port). היציאה יכולה להיות יציאה פיסית בשרת ההדפסה, או יציאה המצביעה לעבר התקן הדפסה ברשת. הגדר רמת עדיפות שונה לכל אחת מהמדפסות הלוגיות המקושרות להתקן ההדפסה ואז, הגדר לקבוצות שונות להשתמש במדפסות לוגיות שונות או הורה למשתמשים לשלוח סוגים שונים של מסמכים למדפסות הלוגיות השונות, בהתאם לרמת העדיפות הנדרשת להם.

איתור וטיפול בתקלות הדפסה שכיחות

כאשר אתה מזהה תקלה בהדפסה, ודא תמיד כי התקן ההדפסה (הברזלים) מחובר כראוי לחשמל, מופעל ומחובר לשרת ההדפסה. במקרה של התקן הדפסה ברשת, ודא כי קיים קשר בין התקן ההדפסה לבין שרת ההדפסה. כדי לקבוע את הגורם לתקלה נסה תחילה להדפיס מתוכנה שונה, כדי לוודא שהבעיה היא במדפסת/התקן ההדפסה ולא בתוכנה עצמה. אם הבעיה אכן במדפסת, שאל את השאלות הבאות:

- ❖ האם משתמשים אחרים יכולים להדפיס כרגיל למדפסת זו ולהתקן הדפסה זה?
- ❖ האם בשרת ההדפסה מותקן מנהל התקן המדפסת (Printer Driver) הנכון עבור התקן ההדפסה (Print Device)?
- ❖ האם שרת ההדפסה פעיל והאם יש בו מספיק מקום פנוי לצורך אגירת עבודות ההדפסה הנשלחות אליו?
- ❖ האם במחשב הלקוח מותקן מנהל ההתקן (Printer Driver) המתאים?
- ❖ האם בשרת ההדפסה מופעלים השירותים Printer Spooler ו- RPC (**R**emote **P**rocedure **C**all)?

מאפייני שרת הדפסה

אם אתה חושד שהבעיה היא בשרת ההדפסה, תוכל לגשת למאפייניו דרך החלון Printers. פתח את תפריט File ובחר באפשרות Server Properties. בתיבת הדו-שיח Print Server Properties תוכל להגדיר גדלי הנייר, יציאות, Printer Drivers והגדרות מתקדמות נוספות, כגון הגדרת תיקיית ההדפסה ברקע (ה-Spooler).

כברירת מחדל מוגדר הנתיב לתיקיית ההדפסה ברקע על ידי Windows 2000 ל- %systemroot%\System32\spool\PRINTERS. אם בשרת הדפסה מתבצעת תעבורה רבה, כדאי לשקול להעביר את תיקיית Spool למחיצה שאינה מחיצת האתחול, ושקיים בה נפח פנוי. אם מחיצת האתחול תתמלא לחלוטין בעבודות הדפסה, ההדפסה תיפסק, וחשוב מכך, מערכת ההפעלה עצמה עלולה להיהפך לבלתי יציבה.

סקירת תקלות הדפסה שכיחות

קיימות מספר תקלות הדפסה שכיחות ברוב סביבות ההדפסה המרושתות. הטבלה הבאה מתארת חלק מאותן תקלות שכיחות, כמו גם גורמים ופתרונות אפשריים :

תקלה	גורם אפשרי	פתרון
המשתמש מקבלת הודעה כי הגישה נדחתה (Access Denied) בעת ניסיון להגדיר את המדפסת מתוך יישום (למשל, גרסאות קודמות של Excel).	למשתמש אין את ההרשאות המתאימות לשינוי הגדרות מדפסת.	שנה את הרשאות המשתמש, או את הגדרת את המדפסת עבורו.
המסמך אינו מודפס בשלמותו, או שפלט המסמך אינו תקין.	מנהל התקן המדפסת אינו מתאים.	התקן את מנהל ההתקן המתאים.
כונן הדיסק הקשיח בשרת ההדפסה עובד ללא הפסק ("טוחן"), משמיע קולות רמים ומסמכים אינם עוברים ממנו להתקן ההדפסה.	אין מספיקי מקום פנוי בדיסק ליצירת קבצי ההדפסה ברקע.	צור מקום פנוי נוסף בשרת ההדפסה או שנה את מיקום תיקיית קבצי ההדפסה ברקע למקום בו יש יותר מקום פנוי.
עמוד הניסיון (Test Page) אינו מודפס. וידאת כי התקן ההדפסה מחובר לחשמל ומופעל.	היציאה הנבחרת אינה נכונה.	הגדר את היציאה הנכונה עבור המדפסת. במקרה של מדפסת המכוונת להתקן הדפסה ברשת ודא כי כתובת הרשת שלה נכונה.

תקלה	גורם אפשרי	פתרון
משתמשים מדווחים כי מופיעה אצלם הודעה המורה להם להתקין מנהל התקן כאשר הם מדפיסים לשרת הדפסה הפועל בסביבת Windows 2000.	בשרת ההדפסה לא מותקנים Printer Drivers עבור הלקוחות.	בשרת ההדפסה, הוסף את מנהלי ההתקן הנדרשים בהתאם לסוג מערכות ההפעלה במחשבי הלקוח. השתמש בתקליטור ההתקנה של מחשב הלקוח, או במנהלי התקנים מיצרן החומרה.
מסמכים שנשלחו להדפסה, מתקבלים אך אינם מודפסים	תור ההדפסה נתקע	יש צורך להפסיק ולהפעיל מחדש את שירות תור ההדפסה (Spool Service).
מסמכים ממחשב לקוח אחד אינם מודפסים, אך מלקוחות אחרים כן.	מחשב הלקוח מחובר למדפסת הלא נכונה.	הסר את המדפסת במחשב הלקוח, ואז התקן מחדש את המדפסת הנכונה.
מסמכים מודפסים כשורה בחלק מהתקני ההדפסה שבמאגר המדפסות, אך לא בכולם.	התקני ההדפסה במאגר המדפסות אינם זהים.	ודא כי כל התקני ההדפסה במאגר המדפסות זהים, או שהם משתמשים באותו מנהל התקן מדפסת. הסר מהמאגר התקנים שאינם תואמים.
מסמכים אינם מודפסים בקדימות המוגדרת להם.	רמות הקדימות בין המדפסות אינן מוגדרות כהלכה.	עדכן את רמות הקדימות במדפסות הלוגיות המשוייכות להתקן ההדפסה.

סיכום שיעור

אתה יכול לבצע גישה למדפסות לצרכי ניהול באחת מהדרכים הבאות: מתוך חלון Printers, תוך שימוש בתוסף התוכנה Active Directory Users and Computers או באמצעות דפדפן אינטרנט. Windows 2000 מאפשרת שליטה בשימוש במדפסות וניהולן על ידי הגדרת הרשאות. ניהול מדפסות כולל הגדרת גודל הנייר בכל אחד ממגשי ההזנה והגדרת דפים מפרידים. בנוסף, תוכל להשהות, להמשיך או לבטל מסמכים בתור ההדפסה, אם מתרחשת תקלה כלשהי בהתקן הדפסה. בנוסף לניהול מדפסות, מאפשרת לך Windows 2000 לנהל גם מסמכים. ניהול מסמכים כולל את השהייתם, המשכתם, התחלת הדפסתם מחדש או ביטולם, במידה ומתרחשת תקלה במסמך המודפס. Windows 2000 מאפשרת ניהול מדפסות מכל מחשב בו מותקן דפדפן אינטרנט, ללא קשר אם מותקנת בו מערכת ההפעלה Windows 2000 או מנהל התקן המדפסת המתאים. Windows 2000 מאפשרת יצירת מאגר מדפסות (Printer Pool), לחיבור מספר רב של התקני הדפסה למדפסת לוגית אחת. מעבר לכך, תוכל גם להגדיר עדיפויות בין מדפסות, כדי ליצור רמות עדיפויות בין קבוצות מסמכים המודפסים לאותו התקן הדפסה. בנוסף לניהול ההדפסה ברשת סקר שיעור זה גם את נושא איתור וטיפול בתקלות הדפסה שכיחות, כגון מסמכים שאינם מודפסים, ומשתמשים שנמנעה מהם הגישה להתקני הדפסה.

שיעור 4: הדפסה ו- Active Directory Services

Active Directory Service אמור להקל על המשתמשים לאתר מדפסות. ב-Windows 2000 תת-מערכת ההדפסה משולבת היטב בשירותי ה- Active Directory – דבר המקל על חיפוש ברחבי ה-Domain אחר מדפסות במיקומים שונים.

לאחר שיעור זה, תוכל

- לתאר כיצד משולבת ההדפסה ב-Active Directory Services.

זמן שיעור משוער: 20 דקות

סקירה כללית של הדפסה ו-Active Directory Services

Active Directory Services הם מסד נתונים מבוזר המשותף בין Domain Controllers ברשת. מידע אודות תורי הדפסה, אתרים, שמות וכתובות נשמר ב-Active Directory Store. מידע זה אמור להישלח על ידי כל שרת הדפסה באופן עצמאי, וזו גם הסיבה לחשיבות עדכון מידע המדפסות ב-Active Directory Store.

מאפיינים רלוונטיים אודות היחסים שבין שרתי ההדפסה לבין שירותי ה- Active Directory כוללים:

- ❖ כל שרת הדפסה אחראי על פרסום המדפסות המותקנות בו ב-Active Directory Store.
- ❖ לשרת ההדפסה אין שייכות ל-DC כלשהו. הוא מאתר DC ב-Domain המתאים באופן דינמי.
- ❖ כאשר מדפסת מעודכנת בשרת ההדפסה, השינויים מופצים מייד ובאופן אוטומטי באמצעות שירותי ה- Active Directory ל- Active Directory Store.
- ❖ מדפסות מפורסמות ב-Active Directory Store כאובייקטים מסוג printQueue. אובייקט printQueue המפורסם, מכיל תת-קבוצה של הנתונים המאוחסנים בשרת ההדפסה אודות המדפסת.

כברירת מחדל, ההדפסה משולבת בשירותי Active Directory כדי שתוכל לפעול ללא התערבות מנהלתית. עליך לערוך שינויים רק במידה שברירת מחדל זו אינה מקובלת עליך.

התנהגות ברירת המחדל כוללת:

- ❖ כל מדפסת המשותפת על ידי שרת הדפסה, מפורסמת באמצעות שירותי Active Directory. הרשאת גישה מנהלתית למחשב המארח (Host) עדיין נדרשת לשם התקנה ושיתוף מדפסת.
- ❖ האובייקט printQueue נשמר באובייקט המחשב (Computer Object) של שרת ההדפסה במחסן Active Directory.

הערה המדפסת אינה מופיעה מתחת לאובייקט Computer שבתוסף התוכנה Active Directory Users And Computers. במקום זאת, שימוש באפשרות Find של תוסף התוכנה Active Directory Users And Computers יציג תוצאה המורה על המדפסת המשוייכת לשרת.

- ❖ כאשר מתבצעים שינויים כלשהם בתצורת המדפסת, אובייקט Active Directory מעודכן. כל נתוני התצורה החדשים נשלחים מחדש למחסן Active Directory, אפילו אם חלקם לא השתנו.
- ❖ אם שרת הדפסה נעלם מהרשת, המדפסות שלו מוסרות משירותי ה-Active Directory.

פרסום Windows 2000 Printers

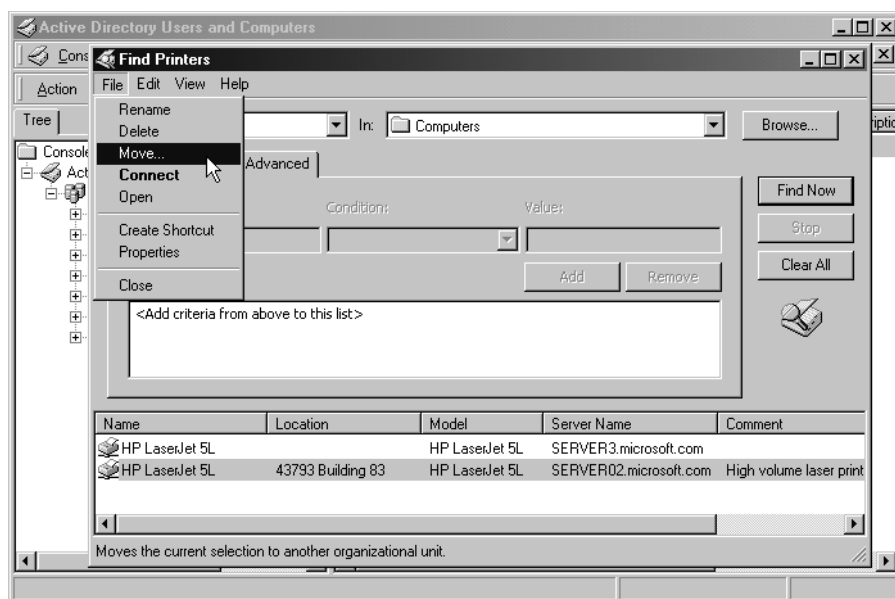
ניתן לפרסם רק מדפסות משותפות (share). פרסום מדפסות נשלט על ידי תיבת הסימון List In The Directory שבכרטיסיה Sharing של מאפייני המדפסת (ראה תרשים 8.7).

האשף Add Printer אינו מאפשר עריכת שינויים בהגדרות אלו בעת יצירת Printer (מדפסת). מדפסות הנוספות באמצעות אשף זה מפורסמות כברירת מחדל. אם אינך מעוניין שמדפסת כלשהי תפורסם בשירות Active Directory, בטל את הסימון בתיבת הסימון List In The Directory בכרטיסיה Sharing שבתיבת הדו-שיח Properties.

כמו כן, ניתן ליצור מדיניות מערכת המונעת פרסום אוטומטי של מדפסות בזמן שיתופן.

הערה רוב הסיכויים הם שהתקן הדפסה המחובר ליציאת אפיק USB -**U**niversal **S**erial **B**us יזוהה אוטומטית, וכתוצאה מכך תותקן עבורו מדפסת לוגית, גם כן באופן אוטומטי. במקרה כזה עליך לשתף ולפרסם את המדפסת באופן ידני באמצעות הכרטיסיה Sharing.

המדפסת (Printer) מוצבת באובייקט המחשב של שרת ההדפסה בשירותי Active Directory. מהרגע שבו היא מוצבת בשירותי Active Directory האובייקט יכול להיות מועבר וניתן לשנות את שמו, מתיבת הדו-שיח Find Printers. לתיבת דו-שיח זו ניתן להגיע מתוך תוסף התוכנה Active Directory Users And Computers. לאחר שפתחת את תוסף התוכנה, פתח את תפריט Action וממנו בחר Find. מהרשימה הנפתחת Find בחר Printers ולחץ על Find Now. תרשים 8.13 מראה כיצד לגשת לאפשרות Move מתוך תיבת הדו-שיח Find Printers.



תרשים 8.13 תיבת הדו-שיח Find Printers המראה כיצד להעביר מדפסת ממקומה.

מנגנון הפרסום

שרת ההדפסה שולח נתונים אסינכרוניים לשירותי Active Directory. ראשית, הוא שולח את הנתונים לאחר השהייה של שנייה אחת. אם פעולה זו נכשלת, מנסה שרת ההדפסה פעם נוספת, כשכל פעם הוא מגדיל את משך ההשהייה, וימשיך כך עד למשך השהייה של שעתיים. עתה, מנסה השרת לשלוח בהשהיה זו עד שיצליח. בשלב המתנה זה מוצגת ההודעה The directory operation is still in progress (פעולת ספריית הרשת עדיין מתנהלת) בכרטיסיה Sharing שבתיבת הדו-שיח Properties של המדפסת.

המדפסת (Printer) מפורסמת ב-DC אקראי, כך ששאילתה עשויה שלא להראות את המדפסת עד שהיא תשוכפל לכל ה-DCs. ל-DCs מקומיים באותו אתר יהיה משך השהייה בערך 30 דקות, אבל בדרך כלל יהיה משך ההשהייה בין 5 ל-10 דקות. לחיפוש בין אתרים שונים, תלוי משך ההשהייה באסטרטגיית השכפול (Replication) הנהוגה בארגון.

Pruning Orphans

כאשר מדפסת נמחקת משרת הדפסה, נמחק גם האובייקט המקביל ב-Active Directory. תוכנה הנקראת Orphan Pruner מבצעת זאת באמצעות פעולה תקופתית על כל DC , כדי לנסות ולאתר אובייקטים של מדפסות שנמחקו. אם מדפסת כבר אינה קיימת, האובייקט נמחק. התוכנה בודקת רק שרתי הדפסה באתר בו פועל ה-DC.

Orphan Pruner נשלטת על ידי מספר הגדרות מדיניות. כברירת מחדל, אם Orphan Pruner אינה מצליחה למצוא את אותה מדפסת שלוש פעמים ברציפות בהפרשי זמן של 8 שעות, היא מניחה כי הרשומה כבר אינה תקפה ומוחקת אותה.

אולם, ייתכנו מצבים בהם המדפסת אינה זמינה, למשל כאשר שרת ההדפסה עובר שדרוג או טיפול תקופתי, או שכובה מסיבה כלשהי, ואז נמחקים האובייקטים, מכיון שה-Active Directory חייב להציג רק את התקני ההדפסה הזמינים כרגע. מרגע שהשרת חוזר לפעילות, צריך לפרסם מחדש (ידנית) את המדפסות שבו. כדי למצות מצב זה, שרת ההדפסה מוודא שהמדפסות שלו מפורסמות כאשר הוא מופעל וכאשר מופעל שירות ההדפסה ברקע, Spooler. ניתן לכפות אתחול הפרסום על ידי הפקודות net stop spooler ו- net start spooler. לחילופין, תוכל להשתמש במדיניות הקבוצתית Check Published State. אפשרות זו נמצאת בתוסף התוכנה Group Policy, בתיקיה Printers, תחת Computer Configuration.

תמיכה במדפסות Windows NT

מדפסות בשרתי הדפסה הפועלים בסביבת Windows NT 4.0 או Windows NT 3.51 יכולות להתפרסם בשירותי Active Directory באמצעות תוסף התוכנה Active Directory Users And Computers. מרגע שהוא נכנס לתוסף התוכנה נוצר אובייקט מדפסת (Printer object) ביחידה ארגונית (**O**rganizational **U**nit - OU), במכולה (Container) או ב-Domain Node, באופן דומה לזה בו נוצרים אובייקטים עבור משתמש או קבוצה. לחילופין, תוכל להשתמש בתסריט (script) Pubprn.vbs אותו תמצא בתיקיה System32. Pubprn.vbs הוא קובץ תסריט של **W**indows **S**cripting **H**ost - WSH ודרושים לו שני פרמטרים. שם המחשב (computer name) של שרת ההדפסה, או שם ה-UNC שלו (\\<computername>\<sharename>) הוא הפרמטר הנדרש הראשון. הפרמטר השני הוא נתיב ה-ADSI, אליו אתה מעוניין שהמידע יפורסם ב-Directory (ספריית הרשת). תוכל לפרסם את כל המדפסות שבשרת או לקבוע מדפסות בודדות שתפורסמנה. לדוגמה, כדי לפרסם באמצעות קובץ התסריט Pubprn.vbs רק את המדפסת המשותפת \\Server03\5L המותקנת בשרת Windows NT ביחידה הארגונית Sales ב-Domain בשם microsoft.com, פתח את חלון שורת הפקודה (Command prompt) והקלד :

```
cscript %systemroot%\system32\pubprn.vbs \\server03\5L
"LDAP:// OU=Sales,DC=microsoft,DC=com"
```

הערה אינך יכול להשתמש בפקודה זו לפרסום מדפסות הפועלות בשרת Windows 2000.

הגדרת מדיניות קבוצתית

שירותי Active Directory כוללים מספר כללי מדיניות קבוצתית המתייחסים לנושא ההדפסה בסביבת Windows 2000. כללי מדיניות אלו נמצאים בצומת Computer Configuration שבתוסף התוכנה Group Policy, תחת ההגדרה Administration Templates. לתיאור מפורט יותר של כל אחד מכללי מדיניות אלו פתח את תיבת הדו-שיח Properties עבור מאפיין מסוים, ובחר בכרטיסיה Explain.

Printer Location Tracking

איתור מיקומי מדפסות ב- Windows 2000 מאפשר למשתמשים לחפש ולמצוא מדפסות (Printers) ב-Loaction שלהם, או ב-Location מוגדר אחר, בהתאם למאפיינים המוגדרים למדפסת. איתור מיקום מאפשר לך לתכנן תרשים מיקום ולשייך מחשבים ומדפסות למיקום מסוים, על פי התכנון. איתור מיקום אוכף את השיטה הסטנדרטית למיקום ושיוך משתמשים ומדפסות, אשר משתמשת בכתובת ה-IP וב-Subnet Mask של המחשב כדי להעריך את מיקומו הפיסי ואת קרבתו למחשבים אחרים. מדיניות הקבוצה Pre-Populate Printer Search Location Text משמשת כדי לאפשר איתור מיקום מדפסת עבור קבוצת מחשבים. למידע נוסף אודות איתור מיקום מדפסות ותהליכים להגדרת האיתור, פנה למערכת העזרה של Windows 2000 Server.

סיכום השיעור

ב-Windows 2000, תת מערכת ההדפסה (Printing Subsystem) משולבת היטב עם שירותי Active Directory, דבר המאפשר לחפש מדפסות (Printers) ב-Domain במיקומים שונים. כברירת מחדל, משולב נושא ההדפסה בשירותי Active Directory, כך שיוכלו לפעול ללא התערבות מנהלתית. כל מדפסת המשותפת על ידי שרת הדפסה מפורסמת בשירותי Active Directory. האובייקט printQueue מוצב באובייקט המחשב של שרת ההדפסה שבשירותי Active Directory. כאשר מתבצעים שינויים כלשהם בהגדרות המדפסת, מעודכן גם האובייקט ב- Active Directory. אם שרת הדפסה נעלם מהרשת, המדפסות שלו מוסרות מה-Active Directory store. ניתן לפרסם רק מדפסות משותפות (Share). פרסום מדפסות נשלט על ידי סימון תיבת הסימון List In The Directory בכרטיסיה Sharing שבתיבת הדו-שיח Properties של המדפסת. בנוסף, מדפסות בשרתי הדפסה הפועלים בסביבת Windows NT 3.51/4.0, יכולות להיות מפורסמות ב-Active Directory Store תוך שימוש בתוסף התוכנה Active Directory Users And Computers, או באמצעות קובץ התסריט Pubprn.vbs. שירותי Active Directory גם כוללים מספר כללי מדיניות קבוצתית אשר אותם ניתן להחיל על הדפסה בסביבת Windows 2000.

שיעור 5: חיבור למדפסת רשת

לאחר שתסיים להגדיר את שרת ההדפסה עם כל מנהלי ההתקנים (Printer Drivers) הדרושים בו עבור כל המדפסות המשותפות, יוכלו משתמשים בעלי מחשבים הפועלים בסביבות מערכות ההפעלה Windows 9x, Windows NT ו-Windows 2000 ליצור בקלות התקשרות למדפסת (Printer) ולהתחיל להדפיס. עבור רוב מחשבי הלקוח מבוססי מערכות הפעלה Windows, מחשב הלקוח מוריד באופן אוטומטי את מנהלי ההתקן (Printer Drivers) עבור המדפסת, בעת שהמשתמש יוצר את ההתחברות הראשונה למדפסת, כל עוד מנהלי ההתקן (Printer Drivers) המתאימים קיימים בשרת ההדפסה.

מחשבי לקוח אחרים, אשר מסוגלים לגשת לשיתוף או להדפיס לכתובת IP, יכולים להדפיס למדפסות המוגדרות כמשותפות בשרת הדפסה מבוסס Windows 2000 Server. האפשרות Connect-to-Printer זמינה רק עבור מחשבי לקוח Windows 9x, Windows NT ו-Windows 2000.

לאחר שיעור זה, תוכל

- ליצור התחברות למדפסת רשת באמצעות האשף Add Printer **או באמצעות דפדפן** האינטרנט.
- לתאר כיצד ניתן להוריד קבצי מנהל התקן (Printer Drivers) עבור מדפסות.

זמן שיעור משוער: 15 דקות

השימוש באשף Add Printer

בעת הוספה ושיתוף של מדפסת (Printer), יכולים כל המשתמשים, כברירת מחדל, להתחבר למדפסת הזו ולהדפיס באמצעותה מסמכים. השיטה ליצירת ההתחברות למחשב הלקוח תלויה במערכת ההפעלה הפועלת בו. מחשבי לקוח הפועלים בסביבת מערכות ההפעלה Windows 9x, Windows NT או Windows 2000 יכולים להשתמש באשף Add Printer שלהם, אם כי האשף Add Printer שמגיע עם Windows 2000 מספק מספר רב יותר של אפשרויות מאשר גרסאותיו הקודמות של אותו אשף. זהו אותו אשף המשמש להוספה ושיתוף של מדפסות. האפשרויות הזמינות באשף אשר מאפשרות לך לאתר ולהתחבר למדפסת, משתנות בהתאם למערכת ההפעלה במחשב הלקוח בו מבוצעת הפעולה.

מחשבי לקוחות הפועלים בסביבת Windows 2000 יכולים גם להשתמש בדפדפן אינטרנט כדי ליצור חיבור למדפסת.

מחשבי לקוח הפועלים בסביבת Windows 2000

השימוש באשף Add Printer במחשבי לקוח הפועלים בסביבת Windows 2000 מאפשר את ביצוע החיבור למדפסת באחד מהאופנים הבאים:

- **חיפוש בשירותי Active Directory** – תוכל לאתר את המדפסת על ידי שימוש באפשרויות החיפוש של שירותי Active Directory. תוכל לבחור לחפש בכל Active Directory Store, או רק בחלק ממנו. תוכל גם לצמצם את החיפוש על ידי ציון קריטריונים, כגון מאפיינים הדרושים לצורך ההדפסה שלך (מדפסת צבע, למשל). דרך קלה לחיפוש היא על ידי לחיצה על Start, הצבעה על Search, ולחיצה על האפשרות For Printers.
- **שימוש בשם UNC** (**U**niversal **N**aming **C**onvention, מוסכמות אוניברסליות למתן שמות) – תוכל להשתמש בשם ה-UNC של המדפסת (\\<print_server>\<share>) כדי ליצור את החיבור - שיטה שיכולה להוכיח את עצמה כמהירה ביותר.
- **עיון ברשת לאיתור המדפסת** – באפשרותך לעיין בתוכן הרשת ולתור אחר מדפסת.

מחשבי לקוח הפועלים בסביבת Windows 9x או Windows NT

במחשבי לקוח הפועלים בסביבת Windows 9x/NT, אשף Add Printer מאפשר הכנסת שם UNC או דפדוף ב- Network Neighborhood כדי לאתר מדפסת.

הערה ניתן לבצע התחברות למדפסת גם באמצעות פקודת Run שבתפריט Start. הקלד את שם UNC של המדפסת בתיבת הטקסט Open ולחץ על OK.

מחשבי לקוח הפועלים בסביבת מערכות הפעלה אחרות של Microsoft

משתמשים במחשבי לקוח בהם פועלת מערכת הפעלה Windows 3.x ו-Windows For Workgroups, משתמשים ב-Print Manager, במקום באשף Add Printer ליצירת חיבור למדפסת.

משתמשים בכל סוג מערכת הפעלה מבוססת Windows יכולים לבצע חיבור למדפסת רשת באמצעות הפקודה הבאה:

```
net use lpt<x>: \\<print_server>\<share>
```

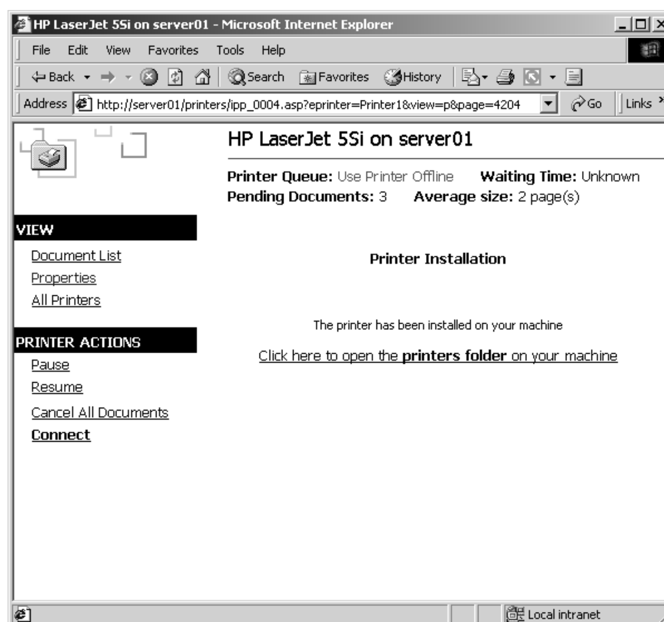
שים לב שהאות x צריכה להיות מוחלפת במספר יציאת המדפסת.

הפקודה net use היא הדרך היחידה ליצירת חיבור למדפסת רשת במחשבים מבוססי MS-DOS או OS/2, כאשר מותקנת בהם תוכנת לקוח Microsoft LAN Manager.

בעת יצירת חיבור באמצעות מערכות הפעלה אלו, לא מתבצעת הורדה אוטומטית של מנהלי ההתקנים (Printer Drivers) תואמים. הפעל את תהליך התקנת מנהלי ההתקנים התואמים במחשב הלקוח המקומי, כפי שהדבר נעשה במערכת ההפעלה המדוברת.

השימוש בדפדפן אינטרנט

אם אתה משתמש במחשב בו מותקנת מערכת ההפעלה Windows 2000, תוכל לבצע את החיבור למדפסת באמצעות רשת האינטרנט של הארגון. תוכל להקליד את כתובת ה-URL - **U**niform **R**esource **L**ocator בדפדפן האינטרנט שלך, ואינך חייב להשתמש באשף Add Printer. בשורת הכתובת של הדפדפן הקלד את כתובת ה-URL של המדפסת http://<print_server>/<share>, ולחץ על הקישור Connect שבדף. תרשים 8.14 מציג את דף האינטרנט המוצג בסיומו של הליך ההתחברות למדפסת.



תרשים 8.14 התחברות והתקנת מדפסת באמצעות דפדפן אינטרנט.

לאחר שביצעת את החיבור מעתיקה Windows 2000 באופן אוטומטי את מנהלי ההתקן (Printer Drivers) התואמים אל מחשב הלקוח.

קיימות שתי כתובות URL בהן תוכל להשתמש ליצירת החיבור למדפסת (Printer) באמצעות דפדפן האינטרנט:

❖ **http://<print_server>/PRINTERS** – הדף שיוצג יציג את כל המדפסות המשותפות בשרת ההדפסה אשר יש לך הרשאה לשימוש בהן. הדף כולל מידע אודות המדפסות, כולל שם המדפסת, מצב עבודות ההדפסה, מיקום, דגם והערות שהוספו כאשר המדפסות הותקנו. מידע זה מסייע לך לבחור את המדפסת הנכונה והמתאימה לצרכיך. מובן שצריכה להיות לך הרשאה לשימוש במדפסת זו.

❖ **http://<print_server>/<share>** – אתה מספק את נתיב האינטראנט למדפסת מסוימת. צריכה להיות לך הרשאה לשימוש במדפסת זו.

תוכל לבצע התאמה אישית של דף האינטרנט המשמש לחיבור מדפסות. לדוגמה, ייתכן שתרצה להציג גם תרשים קומה המציין את מיקומם של התקני ההדפסה אליהם יכולים משתמשים להתחבר.

כדי ששרת הדפסה מבוסס Windows 2000 יוכל לקבל בקשות לביצוע עבודות הדפסה המכילות כתובות URL, הוא חייב להיות מוגדר באחת משתי הדרכים הבאות:

❖ מערכת הפעלה Windows 2000 Server בה מותקן גם IIS.

❖ מערכת הפעלה Windows 2000 Professional בה מותקן גם PWS.

הערה PWS הינה גירסה מצומצמת של IIS.

הורדת מנהלי התקנים עבור מדפסות

כאשר משתמשים במחשבי לקוח בסביבת מערכות ההפעלה Windows 9x/NT/2000 מבצעים את הגישה הראשונה למדפסת בשרת הדפסה, מוריד מחשב הלקוח, באופן אוטומטי, את מנהל ההתקן (Printer Driver) של המדפסת. שרת ההדפסה חייב להכיל העתק של מנהל ההתקן המותקן אצלו. מנהלי התקנים נוספים מותקנים באמצעות לחיצה על לחצן Additional Drivers בכרטיסיה Sharing בתיבת הדו-שיח Properties של המדפסת בשרת.

Printer Drivers הם תלויי פלטפורמה. בשל כך, אם אתה מתעתד לאפשר חיבור למדפסת ממספר מחשבים בפלטפורמות שונות, ודא כי אתה מתקין את כל מנהלי ההתקנים הדרושים לכל הפלטפורמות. לדוגמה, כדי לתמוך במחשבי לקוח מבוססי מעבדי Alpha ומעבדי x86 עליך להתקין את שני סוגים של Printer Drivers בשרת ההדפסה. מנהלי ההתקנים של מחשבים מבוססים Windows NT אינם תואמים לאלה של מחשבים מבוססי Windows 2000. בשל כך, אם אתה מפעיל שרת הדפסה Windows 2000 מבוסס מעבד אינטל x86, ומעוניין לתמוך במחשבי לקוח מבוססי Windows NT, ודא כי אתה מתקין את מנהלי ההתקן עבור מערכות Windows NT מבוססות מעבדי x86. בחלון Additional Drivers תמצא שמנהלי ההתקן המדפסות

מבוססי מעבדי x86 הציבו את Intel בעמודה Environment, אך חשוב לדעת שמנהלי התקנים אלו תומכים גם במעבדי x86 שאינם של Intel.

מחשבי לקוח הפועלים בסביבות Windows NT ו-Windows 2000 מוודאים שמותקן בהם מנהל ההתקן העדכני ביותר בכל פעם שהם שולחים למדפסת עבודת הדפסה. אם מנהל ההתקן (Printer Driver) אינו עדכני, הם יורידו אותו ויעדכנו. למחשבי לקוח אלה עליך לעדכן את מנהלי ההתקנים רק בשרת ההדפסה. מחשבי לקוח מבוססי Windows 9x אינם מחפשים עדכוני Printer Drivers. בלקוחות אלה עליך להתקין את העדכון באופן ידני.

סיכום שיעור

לקוחות בהם פועלת מערכת ההפעלה Windows 9x/NT/2000 יכולים להיעזר באשף Add Printer כדי להתחבר למדפסת. לקוחות Windows 9x/NT יכולים להשתמש בשמות UNC או לדפדף בחלון Network Neighborhood. לקוחות Windows 3.x/WFW משתמשים במנהל ההדפסה (Print Manager) לצורך זה. כל מחשב לקוח מבוסס Windows או MS-DOS יכול להיעזר בפקודה net use כדי להתחבר למדפסת. מחשב לקוח מבוסס Windows 2000 יכול לעיין ב- Active Directory, להשתמש בשמות UNC ולעיין ברשת כדי לאתר מדפסת. מחשבי Windows 2000 יכולים להתחבר למדפסת גם באמצעות דפדפני אינטרנט. כאשר משתמשים במחשבי לקוח Windows 9x/NT/2000 מבצעים התחברות ראשונית לשרת ההדפסה מוריד הלקוח, באופן אוטומטי, את מנהלי ההתקן התואמים עבורו משרת ההדפסה.

שאלות סיכום

השאלות הבאות נועדו לחזק מידע מפתח שהוצג בפרק זה. אם אינך מסוגל לענות על שאלה, עיין בשיעור המתאים ונסה לענות על השאלה פעם נוספת. תשובות לשאלות תמצא בנספח A. לנוחיותך, צרפנו את השאלות באנגלית ואחר כך בעברית.

1. Explain the difference between a print device and a printer.
2. You are told by a colleague never to remove the Everyone system group from the permissions of a printer or no one will be able to manage the printer or its documents. Why is this statement incorrect? How could you configure this undesirable behavior?
3. You have configured two Windows 2000 print servers on your network. When a user connects to one from Windows 95, printing is automatic. When the same user connects to the same print server for a different printer, she gets prompted to install a driver. Why is this happening?
4. In an environment where many users print to the same print device, how can you help reduce the likelihood of users picking up the wrong documents?
5. Can you redirect a single document?
6. A user needs to print a very large document. How can the user print the job after hours without being present while the document prints?

1. הסבר את ההבדל בין התקן הדפסה ומדפסת לוגית.
2. נאמר לך על ידי עמית לעבודה, לעולם לא להסיר את קבוצת המערכת Everyone מהרשאות המדפסת, אחרת אף אחד לא יוכל לנהל את המדפסת ואת המסמכים בה. מדוע הצהרה זו אינה מדויקת? כיצד תוכל להגדיר התנהגות בלתי רצויה זו?
3. הגדרת שני שרתי הדפסה מבוססי Windows 2000 ברשת שלך. כאשר משתמש עם לקוח Windows 95 מתחבר לאחד מהם, ההדפסה מתבצעת באופן אוטומטי. כאשר אותו משתמש מתחבר באותו שרת הדפסה למדפסת שונה, הוא מקבלת הודעה המורה לו להתקין את מנהל ההתקן עבור המדפסת. מדוע זה קורה?
4. כיצד תוכל לסייע להפחית את האפשרות שמשתמשים יקחו בטעות את המסמכים שאינם שלהם, בסביבה בה משתמשים רבים מדפיסים לאותו התקן הדפסה?
5. האם ניתן לנתב מסמך יחיד?
6. משתמש צריך להדפיס מסמך גדול מאוד. כיצד יכול המשתמש להדפיס את עבודתו בשעות שלאחר שעות העבודה מבלי שיהיה נוכח בעת ההדפסה?

פרק 9

פרוטוקולי רשת ושירותים

אודות פרק זה

פרק זה מציג את פרוטוקולי הרשת הנתמכים על ידי Windows 2000, כולל **P**rotocol/**I**nternet **P**rotocol **C**ontrol **T**ransmission (הידוע בקיצור כ- TCP/IP), NWLink, AppleTalk ואחרים. הפרק דן גם בדרכים ליישום פרוטוקול TCP/IP ושירותי רשת נוספים, כגון שירות DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol), את שירות WINS (**W**indows **I**nternet **N**aming **S**ervice), ואת מערכת DNS (**D**omain **N**ame **S**ystem).

לפני שתתחיל

לביצוע השיעורים בפרק זה נדרש :

- ❖ מחשב ובו מותקן ופועל שרת Microsoft 2000.
- ❖ השלמת כל התרגילים בפרקים קודמים.

הערה אין צורך במדפסת כדי להשלים את התרגילים בפרק זה.

שיעור 1: פרוטוקולי רשת

פרוטוקולים הם מפרט ליצירת הסטנדרט של מנות נתונים (Packets of data). הפרוטוקולים מאפשרים שיתוף נתונים ברשת. מנות הנתונים מוזזות מעלה ומטה במחסנית הפרוטוקול (Protocol Stack) ודרך מדיית ההעברה (Transmission Media). Windows 2000 תומכת במיגוון רחב של פרוטוקולים. שיעור זה יציג בפניך את פרוטוקולי הרשת העיקריים, הנתמכים על ידי Windows 2000.

לאחר שיעור זה, תוכל

- לתאר את פרוטוקולי הרשת העיקריים הנתמכים על ידי Windows 2000.

זמן לימוד משוער: 15 דקות

היכרות עם פרוטוקולי רשת

פרוטוקול (Protocol) הוא קבוצת פקודות ומוסכמות לשליחת מידע ברשת (כמו שפה). בין הפרוטוקולים הנתמכים על ידי Windows 2000 תמצא את TCP/IP, עליו מבססת Windows 2000 את תהליך הכניסה לרשת, שירותי קבצים והדפסה, שכפול נתונים בין DCs ומשימות שכיחות נוספות. בנוסף לפרוטוקול TCP/IP הפרוטוקולים העיקריים הנתמכים על ידי Windows 2000 הם:

- **A**synchronous **T**ransfer **M**ode - ATM
- **I**nternet **P**acket E**x**change/**S**equenced **P**acket E**x**change - IPX/SPX
- **NetB**IOS **E**nhanced **U**ser **I**nterface - NetBEUI
- AppleTalk
- **D**ata **L**ink **C**ontrol - DLC
- **I**nfra**r**ed **D**ata **A**ssociation - IrDA

הערה פרוטוקולי SNA (**S**ystem **N**etwork **A**rchitecture) אינם כלולים ב- Windows 2000. פרוטוקולים אלה זמינים באמצעות שרת SNA של Microsoft. שרת SNA הוא מוצר נפרד התומך בשילוב מערכות עם מערכות Midrange ו- Mainframe של IBM.

Protocol Binding Order

פרוטוקולים יכולים להתוסף או להימחק על פי הצורך, ולהיכרך (Binding) באופן סלקטיבי לכל כרטיסי הרשת המותקנים בשרת. Protocol Binding Order נקבע על פי סדר התקנתם של הפרוטוקולים, למרות שהוא ניתן לשינוי בכל עת, על ידי ממשק, דבר המגדיל בהרבה את רמת השליטה. לדוגמה, לכרטיס הרשת הראשון יכולים להיות כרוכים גם פרוטוקול TCP/IP וגם IPX/SPX, כאשר ל-TCP/IP יש קדימות, בעוד שלכרטיס הרשת השני יכולים עדיין אותם שני הפרוטוקולים להיות כרוכים, אך הקדימות תהיה לפרוטוקול IPX/SPX. בנוסף, שירותי רשת יכולים להיות מאופשרים (Enabled) ולא מאופשרים (Disabled) באופן סלקטיבי, על בסיס כרטיס או על בסיס פרוטוקול, או שילוב כלשהו של השניים. סלקטיביות זו מאפשרת למנהל המערכת גמישות רבה בשליטה בתצורות הרישות ומאפשרת הגדרת תצורה בעלת רמת אבטחת מידע גבוהה (למשל, לא לאפשר את כל שירותי הרשת בכרטיס הרשת הציבורי, המחובר ישירות לאינטרנט) ללא טירחה רבה.

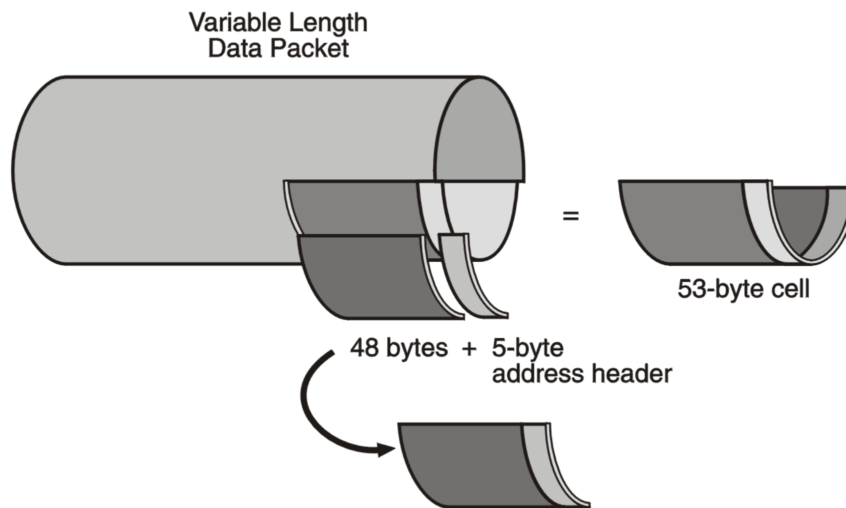
הערה כאשר אנו עובדים עם מספר פרוטוקולים שונים ברשת, מומלץ למקם את הפרוטוקול עם תעבורת הרשת הגדולה ביותר ראשון בסדר ה-Binding.

TCP/IP

חבילת הפרוטוקולים TCP/IP אומצה על ידי Microsoft כפרוטוקול התעבורה עבור Windows 2000. חבילת הפרוטוקול TCP/IP של Windows 2000 נועדה להקל על ההטמעה של רשתות רחבות לארגונים גדולים, מימשל ורשתות ציבוריות, ולספק את היכולת לפעול ברשתות אלו באופן מאובטח. פרוטוקול TCP/IP נדון לעומקו בשיעור 2.

ATM

פרוטוקול ATM (**A**synchronous **T**ransfer **M**ode) הוא יישום מתקדם של מיתוג מנות (Packet Switching), האידיאלי לתקשורת קול, וידאו ונתונים. ATM היא טכנולוגיית רשת מהירה המעבירה נתונים בתאים באורך קבוע. היא מורכבת ממספר טכנולוגיות דומות הכוללות תוכנה, חומרה ותווך מוכוון-חיבור (Connection-Oriented Media). תא (Cell) הוא מנה באורך קבוע של 53 bytes, כמתואר בתרשים 9.1.



תרשים 9.1 מנת נתונים בגודל 1000 בתים מחולקת לתאים בגודל 53 בתים כל אחד.

מאחר שמספר הבתים - וכתוצאה מכך גם זמן ההעברה - הוא קבוע, יכולים התאים להיות מוחלפים במרווחי זמן קבועים.

נקודת הקצה של ATM יוצרת חיבור או מעגל וירטואלי לפני שליחת מידע כלשהו ברשת. אז היא שולחת תאים בנתיב זה לעבר יעדם. המעגל הווירטואלי הוא נתיב ישיר מנקודת קצה אחת לשנייה. בעודה יוצרת את החיבור, עורכת נקודת הקצה גם משא ומתן לגבי איכות השירות (**Q**uality **o**f **S**ervice - QoS) לצורך ההעברה. החוזה המוסכם בעת המשא ומתן כולל את רוחב הפס, השהייה מירבית, מחלוקות מקובלות ופרמטרים אחרים שמספק המעגל הווירטואלי (**V**irtual **C**urcuit - VC), והוא מועבר בין שתי נקודות הקצה. מאחר שהמעגל הווירטואלי הוא מוכוון-חיבור (Connection oriented), מגיעים הנתונים לקצה המקבל, בסדר הנכון ועם רמות שירות ברורות. ATM הוא פשרה מעולה להעברה של קול ונתונים בו-זמנית ברשת. ATM מספק רמת שירות קבועה ומובטחת ברשת מקומית (LAN), רשת מרחבית (WAN) ורשתות ציבוריות.

ארכיטקטורת Windows 2000 עושה שימוש ברכיבים הבאים לצורך תמיכה ב-ATM: הדמיית LAN (LAN Emulation), IP על ATM (IP over ATM), ATM על xDSL (ATM over xDSL) ו-native ATM access באמצעות Winsock 2.0 (Windows Sockets).

LAN Emulation

LAN Emulation (LANE) היא שיטה בה יכולים פרוטוקולים אשר מבינים אך ורק תווך חסר-קישור (Connectionless Media) לתקשר באמצעות ATM. היא מאפשרת ל-ATM לעשות שימוש גם ברשתות ויישומים מיושנים (Legacy Networks and Applications). יישומים ופרוטוקולים מודעי LAN טיפוסיים יכולים לתקשר באמצעות ATM ללא קושי או שינוי.

LANE מכיל שני מרכיבים עיקריים: לקוח LANE (Atmlane.sys) ואת שירותי LANE. לקוח LANE נמצא בתיקיה systemroot%\System32\drivers%. הוא מאפשר לפרוטוקולי LAN וליישומים מודעי-LAN לתפקד, כאילו הם מתקשרים עם LAN טיפוסית. לקוח LANE משדר פקודות LAN לפרוטוקולי הרשת ו-Native ATM commands לשכבת הפרוטוקול ATM. שירותי LANE הם קבוצה של רכיבי ATM, בדרך כלל ממוקמים במתג (Switch) התומך באמולציית LAN.

IP over ATM

IP על ATM היא קבוצת שירותים המשמשת לתקשורת על גבי רשת ATM ואשר יכולה לשמש כתחליף להדמיית LAN. IP על ATM עושה שימוש במאפייני מכווני-קישור (Connection-Oriented) של ATM כדי להתגבר על הטבע חסר הקישור של IP. היא פועלת באופן דומה לפעולת LANE. שרת IP מרכזי (נקרא שרת ATMARP) מחזיק מסד נתונים של כתובות IP וכתובות ATM, ומספק שירותי תצורה ושידור. שירותי שידור אלה דרושים מכיון ש-ATM הוא פרוטוקול שאינו מבצע שידור לכל (Nonbroadcast). שירותי IP על ATM אינם נמצאים במקום אחד, ובדרך כלל לא נמצאים על מתג ATM (ATM Switch). כל שירותי IP על ATM מסופקים עם Windows 2000.

בעצם, IP על ATM היא שכבה קטנה בין פרוטוקול ATM לבין פרוטוקולי TCP/IP. הלקוח מדמה IP תקני לקצהו העליון של פרוטוקול TCP/IP, ומשתמש בפקודות ATM טבעיות (Native) לשכבות ATM שמתחתיו.

IP על ATM מנוהל על ידי שני מרכיבים עיקריים. שרת **A**ddress **R**esolution - ARP **P**rotocol (הקובץ Atmarps.sys) ולקוח ARP (Atmarpc.sys). שרת ARP מורכב משרת ATMARP ושירות MARS (**M**ulticast **A**ddress **R**esolution **S**ervice). שרת ATMARP מספק שירותים המדמים את פעילויות IP הרגילות, בעוד ש-MARS מספק שירותי Broadcast ו-Multicast (שידור לכל ושידור מרובה).

ATM over xDSL

טכנולוגיית xDSL (Digital Subscriber Line) מאפשרת, באמצעות שירות הטלפון הישן והפשוט (**P**lain **O**ld **T**elephone **S**ervice - POTS) לשלוח נתונים דיגיטליים באמצעות חוטי הנחושת הרגילים, לתחנה מרכזית של חברת שירותי הטלפונים. כדי לחבר מספר משתמשי DSL לרשת התשתית של רשת ATM, נשלחים הנתונים למרבב גישה לקו מנוי דיגיטלי (**D**igital **S**ubscriber **L**ine **A**ccess **M**ultiplexer - DSLAM). החלק המרוחק של

DSLAM מחובר לרשת ATM המספקת נפחים בסדרי גודל של גייגה-סיביות (Gigabit). בקצהו השני של כל חיבור פועל מרבב נוסף (DSLAM) אשר תפקידו לפרק את צומת הנתונים ולהעביר אותם לחיבור DSL המסוים אליו נועדו.

ATM על xDSL מאפשרת רשת בגישה מהירה מהבית או ממשרד קטן. סוגים רבים של DSL, הכוללים את קו מנוי דיגיטלי אסימטרי (**A**symmetric **D**igital **S**ubscriber - ADSL **L**ine) ואת קו מנוי דיגיטלי מהיר מאוד (**V**ery high **D**igital **S**ubscriber **L**ine - VDSL), נמצאים בהליך פיתוח ומיועדים לכיוונים אלה. טכנולוגיות אלו משתמשות בלולאה המקומית (Local Loop), קווי הנחושת של ADSL או כבל הסיב האופטי של VDSL, המקשרים בין המשרד המקומי של המשתמש לשקע הנתונים שלו. באזורים רבים מחוברת הלולאה המקומית ישירות לליבת רשת ATM, המופעלת על ידי חברת הטלפונים.

הערה בזק מאפשרת ללקוחותיה חיבור ADSL לחיבור מהיר לאינטרנט

שירות ATM על xDSL משמר את תכונות המהירות הגבוהה ואת הבטחת איכות השירות (QoS Guarantee) שברשת ATM, ללא הצורך לשנות או להחליף פרוטוקולים. דבר זה יוצר פוטנציאל לרשת ATM מקצה-לקצה, למשק הביתי או המשרדי הקטן.

גישה ל-ATM באמצעות Native ATM Access-ו Winsock 2.0

התמיכה של ATM ב- Winsock 2.0 מתאפשרת באמצעות ספק שירותי ATM עבור Windows Socket (Windows Sockets ATM Service Provider). כתוצאה מכך, יישומים הנעזרים בפרוטוקול TCP כפרוטוקול ההעברה שלהם, יכולים להשתמש ישירות ב- Winsock 2.0 כדי לבצע גישה לרשת מבוססת ATM.

יישומים המשתמשים ב-ATM טבעית (Native ATM) יכולים ליצור מעגלים וירטואליים וגישה להבטחות איכות שירות (QoS Guarantees). תכונה זו מסופקת על ידי שירות מבוסס-חיבור המוסף לגירסה 5.0 של שירות ממשק מנהל-התקן-הרשת (NDIS - **N**etwork **D**river **I**nterface **S**ervice). שירות מכוון-קישור של NDIS 5.0 נקרא CoNDIS.

NWLink

NWLink הוא יישום של פרוטוקול IPX/SPX מבית Novell NetWare שבוצע על ידי Microsoft. NWLink משמש לרוב בסביבות בהן קיימים לקוחות המפעילים מערכות הפעלה של Microsoft אשר משמשות לקבלת שירותים בשרתי NetWare, או במקום בו פועלים לקוחות NetWare אשר משמשים לצורך גישה למשאבים הנמצאים בשרתים הפועלים בסביבת מערכות הפעלה של Microsoft. NWLink לבדו אינו מאפשר למחשב הפועל בסביבת Windows 2000 לבצע גישה ישירה לקבצים או מדפסות המשותפים בשרתי NetWare, או לשמש כשרת קבצים או הדפסה ללקוחות NetWare. כדי לגשת לקבצים או מדפסות בשרת NetWare יש להשתמש בשירות ייעודי, כגון שירות לקוח

עבור NetWare (**C**lient **S**ervice for **N**et**W**are - CSNW) הנמצא ב- Windows 2000 Professional או שירות שער עבור NetWare (**G**ateway **S**ervice for **N**et**W**are - GSNW) הנמצא ב- Windows 2000 Server.

GSNW משמש כשירות לקוח המאפשר גישה למשאבי שרת NetWare עבור מחשב המפעיל שרת Windows 2000, כאשר הוא מותקן בו, וכגשר (Gateway) עבור מחשבי לקוח אחרים המבקשים גישה למשאבי שרת NetWare באמצעות שרת Windows 2000. פונקציית הגשר מאפשרת לשרת Windows 2000 לשתף משאבי NetWare (קבצים ומדפסות) ממש כאילו היו ממוקמים בשרת Windows 2000. כתוצאה מכך, מחשבי לקוח אשר יכולים לגשת לשיתופים בשרת Windows 2000 יכולים להשתמש בשיתופים הזמינים דרך GSNW. GSNW הוא פתרון גישה בעל רמת ביצועים נמוכה; הוא מאפשר גישור של חיבור משתמש בודד למשאבים בשרת NetWare.

NWLink יעיל אם קיימים ופעילים יישומי שרת/לקוח של NetWare, המשתמשים בפרוטוקולים Winsock או NetBIOS over IPX/SPX. בנוסף, **N**et**W**are **N**et**B**IOS **Link** (NWNBLink) מכיל הרחבות של Microsoft עבור NetBIOS. רכיב NWNBLink משמש לעיצוב בקשות ברמת NetBIOS והעברתם לרכיב NWLink, לצורך העברה ברשת.

הגדרת סוג מסגרת

סוג המסגרת (Frame Type) מגדיר את האופן בו כרטיס רשת (network adapter), במחשב מבוסס Windows 2000, מעצב את הנתונים לשליחה ברשת. כדי לתקשר בין מחשב Windows 2000 ושרתי NetWare עליך להגדיר את NWLink במחשב Windows 2000 לאותו סוג מסגרת כמו זה המוגדר בשרתי NetWare. הטבלה הבאה מציגה רשימת טכנולוגיות רשת ואת סוגי המסגרות הנתמכות על ידי NWLink:

טכנולוגיית רשת	סוגי מסגרות נתמכות
Ethernet	Ethernet II, 802.3, 802.2 ופרוטוקול גישה לרשת משנה (SNAP - Sub Network Access Protocol) אשר ברירת המחדל שלו היא 802.2.
Token Ring	802.5 ו-SNAP
FDDI - Fiber Distributed Data Interface	802.2 ו- 802.3

ברשתות Ethernet, סוג המסגרת התקנית עבור NetWare גרסאות 2.2-3.11 הוא 802.3. החל בגירסה 3.12 של NetWare הומר סוג המסגרת התקני ל- 802.2.

באפשרותך לבחור בין זיהוי אוטומטי של סוג המסגרת לבין הגדרה ידנית שלה. אולם, אם סוג המסגרת מזוהה באופן אוטומטי ברגע שנטען NWLink ומזוהים מספר סוגי מסגרות בנוסף לסוג מסגרת 802.2, NWLink עובר לברירת מחדל של סוג מסגרת 802.2. במקרה זה, לא יוכל Windows 2000 לתקשר עם שרתי NetWare הפועלים עם מסגרות אחרות כגון 802.3.

אם סוג המסגרת מוגדר באופן ידני, מחשב שבו פועלת מערכת ההפעלה Windows 2000 יכול להשתמש בריבוי סוגי מסגרות, בו-זמנית.

את סוג המסגרת ניתן להגדיר בתיבת הדו-שיח -
NWLink IPX/SPX/NetBIOS-Compatible Transport Protocol Properties.

למידע נוסף פנה למערכת העזרה של Windows 2000.

NetBEUI

NetBEUI פותח במקורו כפרוטוקול עבור רשתות LAN מחלקתיות, של בין 20 ועד 200 מחשבים. NetBEUI הוא פרוטוקול חסר-ניתוב (Nonroutable) מכיון שאינו כולל את שכבת הרשת (Network Layer). בשל מגבלה זו עליך לחבר מחשבים הפועלים בסביבת Windows 2000 ופרוטוקול NetBEUI באמצעות גשרים (Bridges), במקום נתבים (Routers). בנוסף, NetBEUI הוא פרוטוקול מבוסס-שידור לכל (Broadcast). משמעות הדבר היא שהפרוטוקול מסתמך על שידור Broadcast עבור רוב פעילויותיו, כגון רישום שמות (Name Registration) וגילוי (Discovery), וכך יוצר יותר תעבורת שידור ברשת מפרוטוקולים אחרים. NetBEUI נכלל ב- Windows 2000 Professional וב-Windows 2000 Server רק לשם התאימות לאחור, כדי לתמוך בתחנות עבודה שעדיין לא שודרגו ל- Windows 2000.

NetBEUI מאפשר תאימות עם רשתות מקומיות קיימות, המשתמשות בפרוטוקול זה. הוא מאפשר למחשבי Windows 2000 :

- תקשורת מכוונת-קישור (Connection-Oriented) וחסרת קישור (Connectionless) בין מחשבים.
- הגדרת תצורה עצמית וכיוונון עצמי.
- הגנה בפני שגיאות.
- תקורת זיכרון נמוכה.

הערה רשת Windows 2000 המפעילה את **שירותי** Active Directory **אינה יכולה להשתמש ב-**NWLink **או ב-**NetBEUI **כפרוטוקול הראשי בה. לצורך הגישה לשירות** Active Directory **יכול לשמש רק פרוטוקול** TCP/IP.

AppleTalk

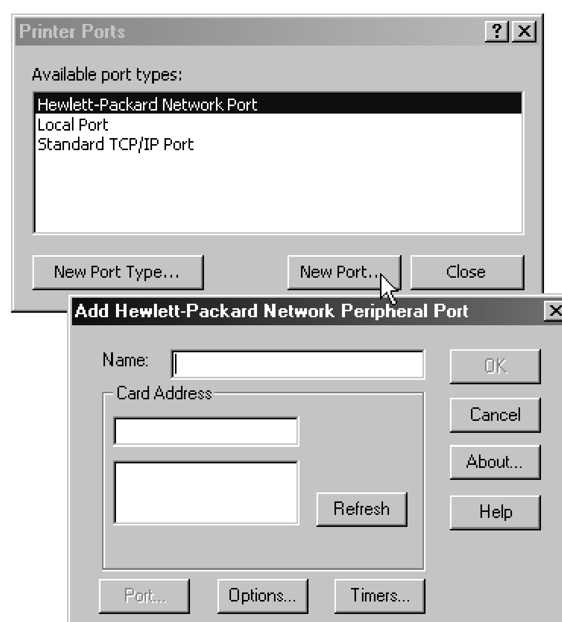
פרוטוקול AppleTalk הוא למעשה חבילת פרוטוקולים שפותחה על ידי Apple Computer Corporation לצורך תקשורת בין מחשבי מקינטוש. Windows 2000 כוללת תמיכה עבור AppleTalk, דבר המאפשר לשרתי Windows 2000 וללקוחות מקינטוש לשתף קבצים ותיקיות. AppleTalk גם מאפשר למחשב Windows 2000 לשמש כנתב (Router) וכשרת גישה בחיוג (Dial-up Server).

כדי שפרוטוקול AppleTalk יפעל כהלכה, חייב להיות ברשת שרת Windows 2000 פעיל וזמין, המוגדר להפעיל את שירותי מקינטוש (Windows 2000 Services for Macintosh).

DLC

פרוטוקול DLC פותח לצרכי תקשורת Mainframe של IBM. הוא לא נועד להיות פרוטוקול עיקרי ברשת המבוססת על מחשבים אישיים. אולם, DLC משמש להדפסה למדפסות מבית Hewlett-Packard המחוברות ישירות לרשתות. מדפסות המחוברות לרשת משתמשות בפרוטוקול DLC, מכיון שהמסגרות המתקבלות ניתנות לפירוק בקלות, ומכיון שתפקודיות DLC ניתנת לקידוד קל לזיכרון לקריאה בלבד (ROM). התועלת של DLC מוגבלת, מפני שאינו צריך להתממשק ישירות עם שכבת ממשק מנהל התקן ההעברה (Transport Driver Interface). את פרוטוקול DLC יש להתקין אך ורק במחשבים ברשת המבצעים משימות, כגון שליחת נתונים למדפסות רשת מתוצרת Hewlett-Packard. לקוחות השולחים עבודות הדפסה להתקן הדפסה ברשת באמצעות שרת הדפסה מבוסס Windows 2000 אינם צריכים שיהיה מותקן בהם פרוטוקול DLC.

פרוטוקול DLC חייב להיות מותקן רק בשרת ההדפסה המתקשר ישירות עם התקן ההדפסה. לאחר שיותקן פרוטוקול DLC בשרת הדפסה מבוסס Windows 2000, ייווצר בשרת סוג חדש של יציאת מדפסת. תרשים 9.2 מציג את סוג היציאה החדש, כפי שמופיע בתיבת הדו-שיח Printer Port. לתיבת דו-שיח זו ניגשים מהכרטיסיה Ports שבתיבת הדו-שיח של מאפייני המדפסת.



תרשים 9.2 תיבת הדו-שיח המשמשת להגדרת מדפסת רשת Hewlett-Packard חדשה מבוססת DLC.

כתובת ה-MAC (**M**edia **A**ccess **C**ontrol) של כרטיס הרשת עבור מדפסות שרתי הדפסה DLC, מופיעה בתיבה הגדולה יותר שמתחת ל- Card Address (ראה תרשים 9.2). ודא שהתקן ההדפסה ברשת התומך DLC מחובר לרשת, מופעל ומוגדר לעבודה עם DLC.

לאחר שהגדרת את שרת Windows 2000 לשמש כשרת הדפסה עבור התקן הדפסה ברשת התומך DLC, יכולים מחשבי לקוח להתחבר לשיתוף בשרת Windows 2000. אם בהתקן ההדפסה התומך DLC מופיעות עבודות הדפסה שלא נשלחו דרך שרת ההדפסה, ייתכן שבמחשבי הלקוחות מותקן פרוטוקול DLC והם מדפיסים ישירות להתקן ההדפסה. היעזר בכלי Network Monitor, או כל כלי אבחון אחר, כדי לקבוע איזה מחשבים ברשת מפעילים את פרוטוקול DLC.

הערה נכון לכתיבת שורות אלו, כל כרטיסי Hewlett-Packard JetDirect **תומכים בפרוטוקול** TCP/IP **ויש להוסיפם תוך שימוש באפשרות** Standard TCP/IP Port. **רק כרטיסי** Hewlett-Packard JetDirect **מיושנים - כאלה שאינם תומכים בפרוטוקול** TCP/IP, **דורשים את יציאת הרשת העושה שימוש בפרוטוקול** DLC.

IrDA

פרוטוקול IrDA הוא למעשה קבוצת פרוטוקולים. זהו פרוטוקול לטווח קצר, מהיר מאוד, דו-כיווני, אלחוטי בתקשורת אינפרא-אדומה. IrDA מאפשר למיגוון התקנים לתקשר ביניהם, כגון מצלמות, מדפסות, מחשבים ניידים, מחשבים שולחניים ומנהלי מידע אישיים (**P**ersonal **D**ata **A**ssistants - PDA). מחסנית פרוטוקול IrDA נגישה באמצעות מנהלי ההתקן חסרי-החיבור של NDIS.

סיכום שיעור

פרוטוקול הוא קבוצת חוקים לשליחת נתונים ברשת. Windows 2000 תומכת במספר פרוטוקולים, ביניהם TCP/IP. חבילת הפרוטוקולים TCP/IP אומצה על ידי Microsoft כפרוטוקול ההעברה האסטרטגי עבור ארגונים בסביבת Windows 2000. פרוטוקול TCP/IP יכול להיות מועבר בין מספר רשתות המבוססות על טכנולוגיות תווכי גישה כגון Ethernet, Token Ring ו-ATM. תווך גישה (Media Access) הוא רק חלק ממה שמספק ATM. ATM היא קבוצת טכנולוגיות (חומרה ותוכנה) אשר יחדיו מאפשרים תקשורת מכוונת-שידור, האידיאלית לצרכי העברת קול, וידאו ותקשורת נתונים. NWLink הוא פרוטוקול של Microsoft התואם לפרוטוקול IPX/SPX של חברת Novell, עבור Windows 2000. NetBEUI גם הוא נכלל עם Windows 2000 Server ועם Windows 2000 Professional, למרות שהוא פרוטוקול מיושן, שנועד בעיקרו לתמוך בתחנות שעדיין לא עברו שדרוג ל-Windows 2000. בנוסף, Windows 2000 כוללת תמיכה ב-AppleTalk, מה שמאפשר למחשב Windows 2000 לשמש גם כנתב (Router) ושרת חיוג (Dial-up Server). DLC פותח עבור מחשבי Mainframe של IBM; התקני הדפסה ברשת מיושנים של Hewlett-Packard מתחברים לרשת באמצעות פרוטוקול DLC. IrDA הוא קבוצת פרוטוקולים לטווח קצר, מהירים מאוד, דו-כיווניים, אלחוטיים בתקשורת אינפרא-אדומה.

שיעור 2: TCP/IP

פרוטוקול TCP/IP מאפשר תקשורת ברשתות המכילות מחשבים בהם ארכיטקטורות חומרה שונות ומיגוון מערכות הפעלה. יישומה של Microsoft לפרוטוקול TCP/IP מאפשר רישות ארגוני וקישוריות בין מחשבים מבוססי Windows 2000.

לאחר שיעור זה, תוכל

- **לתאר את חבילת פרוטוקולי הרשת** TCP/IP**, ואת תוכניות השירות עבור** TCP/IP **המשווקות עם** Windows 2000**.**
- **להגדיר** TCP/IP**.**

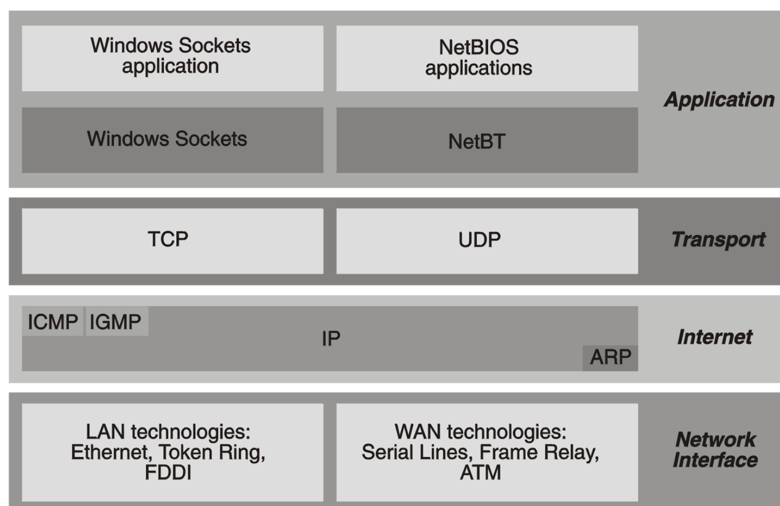
זמן לימוד משוער: 60 דקות

סקירה של חבילת TCP/IP

פרוטוקול TCP/IP הוא למעשה חבילת פרוטוקולים תקנית בתעשיית המחשבים המאפשרת רישות ארגוני וקישוריות בין מחשבים מבוססי Windows 2000. הוספת TCP/IP לתצורת Windows 2000 מציעה את היתרונות הבאים:

- ❖ פרוטוקול רשת מנותב (Routable) אשר נתמך על ידי רוב מערכות ההפעלה. רוב הרשתות הגדולות מתבססות על פרוטוקול TCP/IP, כולל רשת האינטרנט.
- ❖ טכנולוגיה לקישור בין מערכות שונות. ניתן להשתמש במיגוון רחב של תוכניות שירות להתחברות כדי לגשת ולהעביר מידע (נתונים) בין מערכות שונות. Windows 2000 כוללת חלק מתוכניות שירות אלו.
- ❖ מסגרת שרת/לקוח איתנה, המאפשרת צמיחה ותומכת במיגוון פלטפורמות. TCP/IP תומך בממשק Winsock, הנחשב לאידיאלי לצרכי פיתוח יישומי שרת/לקוח למחסניות תואמות Winsock.
- ❖ שיטה לקבלת גישה למשאבי אינטרנט.

חבילת הפרוטוקולים TCP/IP מספקת קבוצת תקנים לגבי האופן בו מחשבים מתקשרים וכיצד רשתות מתחברות ביניהן. חבילת TCP/IP ממופה למודל סטנדרטי בן ארבע שכבות: **ממשק רשת** (Network Interface), **אינטרנט** (Internet), **העברה** (Transport) **ויישומים** (Application), ראה תרשים 9.3.



תרשים 9.3 חבילת הפרוטוקולים TCP/IP בחלוקה לארבע שכבות.

Network Interface Layer

בבסיס של המודל תמצא את שכבת ממשק הרשת (Network Interface layer). שכבה זו שמה את מסגרות המידע על חוט התקשורת הפיסי ומושכת מסגרות מהחוט.

Internet Layer

פרוטוקולי שכבת האינטרנט (Internet layer) מאגדים מנות לצרורות נתונים (Internet Datagram) ומבצעים את כל האלגוריתמים של הניתוב הנדרשים. ארבעה פרוטוקולי שכבת האינטרנט העיקריים הם: IP - **I**nternet **P**rotocol, ARP - **A**ddress **R**esolution **P**rotocol, ICMP - **I**nternet **C**ontrol **M**essage **P**rotocol ו- IGMP - **I**nternet **G**roup **M**anagement **P**rotocol.

הטבלה הבאה מתארת את ארבעת הפרוטוקולים הללו:

פרוטוקול	תיאור
IP	מבצע משלוח מנות חסר-קישור לכל הפרוטוקולים האחרים בחבילה. אינו מבטיח הגעתה של מנה או את סדר הגעתן הנכון של המנות.
ARP	מבצע מיפוי כתובת IP (כתובת לוגית) לכתובת שכבת המשנהשל MAC (כתובת פיסית), כדי להשיג את כתובת ה-MAC המזהה של היעד. IP משדר מנת שאילתת ARP מיוחדת, המכילה את כתובת ה-IP של מחשב היעד. המחשב שכתובת ה-IP שלו תואמת לכתובת בשאילתה עונה על ידי שליחת כתובתו הפיסית למבקש. שכבת המשנה של ה-MAC מתקשרת ישירות עם כרטיס מתאם הרשת והיא אחראית על שליחה ללא תקלות של הנתונים בין שני המחשבים ברשת.

פרוטוקול	תיאור
ICMP	מבצע תקשורת מיוחדת בין מארחים (Hosts), ובכך מאפשר להם לשתף ביניהם נתוני מצב ושגיאות. פרוטוקולים ברמה גבוהה יותר נעזרים בנתונים אלה כדי להתאושש מבעיות העברה. מנהלי רשת משתמשים בנתונים אלה כדי לזהות תקלות ברשת. תוכנית השירות PING משתמשת במנות ICMP כדי לקבוע אם התקן IP כלשהו ברשת פעיל ומתפקד.
IGMP	מבצע Multicasting, שהוא גירסה מוגבלת של Broadcasting, כדי לתקשר ולנהל נתונים בהתקנים החברים בקבוצת ה-Multicast. IGMP מדווח לנתבי Multicast שכנים אודות חברויות קבוצות האירוח ברשת מסוימת. Windows 2000 תומכת באפשרויות Multicast, כגון שירותי NetShow של שרת Windows 2000 (Windows 2000 Server NetShow Services), אשר מאפשרות למפתחים ליצור תוכניות Multicast.

Transport Layer

פרוטוקולי שכבת ההעברה (Transport Layer) מבצעים Communication Session (התקשרות) בין מחשבים. שיטת שליחת הנתונים המועדפת קובעת את פרוטוקול ההעברה. שני פרוטוקולי שכבת ההעברה הם: TCP (**T**ransmission **C**ontrol **P**rotocol) ו- UDP (**U**ser **D**atagram **P**rotocol).

הטבלה הבאה מתארת את שני הפרוטוקולים:

פרוטוקול	תיאור
TCP	מבצע תקשורת אמינה מכוונת-קישור (Connection-Oriented) עבור יישומים שבדרך כלל מעבירים כמות גדולה של נתונים בבת אחת, או כאלה הדורשים אישור על כך שהנתונים הגיעו ליעדם. TCP מבטיח את משלוח המנות, מבטיח את סדר הגעתן ומבצע בדיקת סכום (Checksum) המאשרת כי כותרת המנה ותוכנה תקינים.
UDP	מבצע תקשורת חסרת-קישור (Connectionless) ואינו מבטיח את הגעתן של המנות. יישומים העושים שימוש ב-UDP בדרך כלל מעבירים כמויות קטנות של נתונים בבת אחת. אמינות ההעברה היא באחריותו של היישום. לדוגמה: שידור רדיו באינטרנט.

Application Layer

בראש המודל נמצאת שכבת היישום (Application Layer), אשר באמצעותה משיגים היישומים את הגישה לרשת. בשכבה זו קיימות תוכניות שירות ושירותים רבים לנושא TCP/IP, כגון FTP, Telnet, SNMP (**S**imple **N**etwork **M**anagement **P**rotocol), DNS וכדומה.

TCP/IP מספק ליישומי רשת שני ממשקים, שישתמשו בשירותי מחסנית פרוטוקול TCP/IP: ממשק Winsock וממשק NetBIOS over TCP/IP (NetBT). הטבלה הבאה מתארת את שני ממשקים אלה:

ממשק	תיאור
Winsock	משמש כממשק תקני בין יישומים מבוססי Socket ופרוטוקולי TCP/IP.
NetBT	משמש כממשק תקני עבור שירותי NetBIOS, כולל שם (Name), צרור נתונים (Datagram) ו-Session Services. הוא גם משמש כממשק תקני בין יישומים מבוססי NetBIOS ופרוטוקולי TCP/IP.

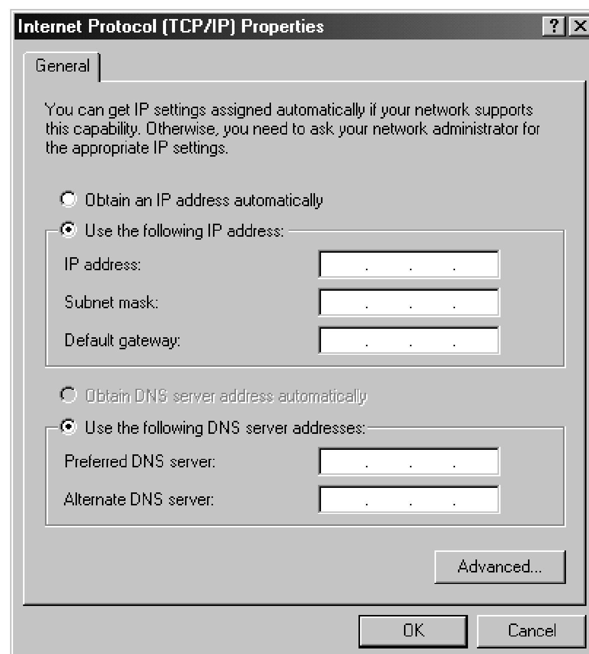
הערה למידע נוסף אודות TCP/IP ואודות יישום TCP/IP פנה לתקליטור המצורף לספר זה (\chapt09\articles\tcpip2000.doc).

הגדרת TCP/IP לשימוש בכתובת IP קבועה

כברירת מחדל, מחשבי לקוח הפועלים עם מערכות ההפעלה Windows 2000, Windows NT או Windows 9x, משיגים באופן אוטומטי את נתוני תצורת TCP/IP באמצעות שירות DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol). אך אפילו בסביבה בה מופעל שירות DHCP, עליך להגדיר למספר מחשבים ברשת כתובת IP קבועה (Static IP Address). לדוגמה, מחשב המחזיק ומפעיל את שירות DHCP אינו יכול להיות לקוח DHCP, כך שצריכה להיות לו כתובת IP קבועה. אם שירות DHCP אינו זמין, עליך גם להגדיר את TCP/IP כך שישתמש בכתובת IP קבועה.

הערה ברשתות קטנות פרטיות בהן אין שרת DHCP זמין, אתה יכול להשתמש בשירות פנימי של Windows 2000 הנקרא **A**utomatic **P**rivate **IP** **A**ddressing (APIPA, מיעון IP פרטי אוטומטי) כדי להגדיר כתובות IP עבורך באופן אוטומטי. שירות זה מתואר בהמשך שיעור זה.

לכל כרטיס מתאם רשת המותקן במחשב ומשתמש ב-TCP/IP, תוכל להגדיר כתובת IP, Subnet Mask ו-Default Gateway, כפי שמוצג בתרשים 9.4.



תרשים 9.4 הגדרת כתובת IP קבועה בתיבת הדו-שיח Internet Protocol (TCP/IP) Properties

הטבלה הבאה מתארת את האפשרויות בעת הגדרת כתובת TCP/IP קבועה.

אפשרות	תיאור
IP Address	כתובת לוגית בת 32 סיביות המזהה את מארח TCP/IP.כל כרטיס מתאם רשת המותקן במחשב ומפעיל את TCP/IP חייב כתובת IP ייחודית, כגון 192.168.0.108. לכל כתובת שני חלקים: **מזהה רשת** (Network ID), המזהה את כל המארחים באותה רשת פיסית, **ומזהה מארח** (Host ID), המזהה מארח מסוים ברשת. בדוגמה זו, מזהה הרשת הוא 192.168.0 ומזהה המארח הוא 108.
Subnet Mask	רשת בסביבה מרובת-רשתות אשר עושה שימוש בכתובות IP הנגזרות ממזהה רשת יחיד. רשתות משנה מחלקות רשת גדולה למספר רשתות פיסיות המחוברות באמצעות נתבים (Routers). Subnet Mask חוסמת חלק מכתובת ה-IP באופן כזה ש- TCP/IP יוכל להבדיל בין מזהה הרשת למזהה המארח. כאשר מארחי TCP/IP מנסים לתקשר, קובעת רשת המשנה האם מארח היעד שייך לרשת המקומית, או שהוא שייך לרשת מרוחקת. כדי לתקשר בתחומי הרשת המקומית צריכים המחשבים שתהיה מוגדרת להם כתובת Subnet Mask זהה וכתובת מזהה רשת זהה. זהו בעצם מקרא לכתובת IP כדי לבצע מיסוך בין מזהה הרשת ומזהה המארח בכתובת IP נתונה.

אפשרות	תיאור
Default Gateway	ההתקן המתווך ברשת המקומית אשר מאחסן את מזהי הרשת של רשתות אחרות בארגון, או באינטרנט. כדי לתקשר עם מארח ברשת מרוחקת, יש להגדיר כתובת IP עבור Default Gateway. TCP/IP שולח מנות המיועדות לרשתות מרוחקות אל Default Gateway (אם לא הוגדר לו נתב אחר), המאפשר להעביר את המנות לשערים אחרים, עד שהמנה מגיעה לאותו שער מרוחק אליו מחובר היעד הרצוי. כאשר יש נתב המפריד בין חלקי הרשת השונים, חובה לציין למחשב את כתובת ה-IP של הנתב, אחרת לא ניתן יהיה לתקשר עם רשתות מרוחקות. כתובת IP של נתב מקומי נקראת כתובת Default Gateway.

כדי לפתוח את תיבת הדו-שיח Internet Protocol (TCP/IP) Properties יש קודם כל לפתוח את תיבת המאפיינים של My Network Places, אחר כך לפתוח את מאפייני כרטיס מתאם הרשת המבוקש, ואז לפתוח את תיבת הדו-שיח Internet Protocol (TCP/IP) Properties עבור הרכיב Internet Protocol (TCP/IP).

אזהרה תקשורת IP יכולה להיכשל אם קיימת כפילות כתובות IP ברשת. בשל כך, לפני שתגדיר כתובת IP קבועה עליך תמיד לבדוק עם מנהל הרשת מהן הכתובות הזמינות.

הגדרת TCP/IP לקבלת כתובת IP באופן אוטומטי

אם ברשת קיים (וזמין) מחשב המפעיל את שירות DHCP, הוא יכול להקצות באופן אוטומטי נתוני תצורת TCP/IP ללקוח DHCP. אז, תוכל להגדיר לכל הלקוחות הפועלים בסביבת MS-DOS או Windows 3.x/9x/NT/2000 לקבל את הקצאת נתוני TCP/IP באופן אוטומטי משירות DHCP הפעיל. השימוש ב-DHCP להגדרה אוטומטית של נתוני TCP/IP במחשב לקוח יכול לפשט את נושא ניהול הקצאת הכתובות ולהבטיח נתוני תצורה מדויקים. אבל לפני שתוכל להגדיר את שירות DHCP, כך שיספק ללקוחות הרשת את נתוני תצורת TCP/IP באופן אוטומטי, עליך להגדיר מחשב כלקוח DHCP.

כדי להגדיר לקוח DHCP פתח את תיבת הדו-שיח Internet Protocol (TCP/IP) Properties ולחץ על לחצן האפשרויות Obtain an IP address automatically. נושא DHCP מתואר ביתר פירוט בשיעור 3 ״DHCP״.

Automatic Private IP Addressing

יישום TCP/IP במערכת ההפעלה Windows 2000 תומך במנגנון חדש למיעון אוטומטי של כתובות IP, המיועד לתצורות פשוטות של רשתות LAN. מנגנון מיעון זה הוא הרחבה של הקצאת הכתובות האוטומטית לכרטיסי LAN, ומאפשר הגדרת כתובות IP ללא הצורך להקצות כתובות IP קבועות או להתקין את שירות DHCP.

כדי שהמאפיין **A**utomatic **P**rivate **IP A**ddressing - APIPA יפעל כהלכה במחשב הפועל בסביבת Windows 2000, עליך להגדיר כרטיס מתאם רשת LAN לשימוש ב-TCP/IP ובתיבת הדו-שיח Internet Protocol (TCP/IP) Properties ללחוץ על לחצן האפשרויות Obtain an IP address automatically.

הצעדים הבאים מתארים כיצד מקצה APIPA כתובת IP :

1. TCP/IP של Windows 2000 מנסה למצוא שרת DHCP ברשת הקרובה, כדי לקבל הקצאה דינמית של כתובת IP.
2. מכיון שבעת תהליך האתחול לא אותר שרת DHCP (לדוגמה, אם השרת "ירד" לצרכי תחזוקה), הלקוח אינו יכול לקבל כתובת IP אוטומטית משרת DHCP.
3. APIPA מחולל כתובת IP במבנה 169.254.x.y (כאשר x.y הוא המזהה הייחודי של המארח) ו-subnet mask מוגדרת לערך 255.255.0.0. אם הכתובת נמצאת בשימוש, APIPA מחולל כתובת אחרת, ואם צריך, יבצע זאת שוב ושוב, עד 10 פעמים.

הערה הרשות להקצאת מספרי אינטרנט (**I**nternet **A**ssigned **N**umbers **A**uthority - IANA) קבעה כי טווח הכתובות 169.254.0.0 ועד 169.254.255.255 יישמר עבור שירותי מיעון IP פרטי אוטומטי (Automatic Private IP Addressing). כך, מובטח לך כי הכתובת המוקצית ללקוח באמצעות APIPA לא תגרום להתנגשות בין כתובות מנותבות (Routable).

לאחר שהמחשב מחולל את הכתובת, הוא משדר אותה. אם אף מחשב אחר ברשת לא הגיב לשידור אז הוא מקצה אותה לעצמו. המחשב ימשיך להשתמש בכתובת זו עד שיזהה ויקבל נתוני הגדרת תצורה משרת DHCP. דבר זה מאפשר לשני מחשבים המחוברים לרכזת LAN לאתחל ללא כל הגדרת כתובת IP, ולהמשיך ולהשתמש בפרוטוקול TCP/IP לצרכי התקשורת המקומיים.

הערה גם Windows 98 תומכת ב-APIPA.

למרות ש-APIPA יכול להקצות באופן אוטומטי כתובות IP ללקוחות DHCP, הוא אינו מחולל את כל הנתונים אשר מסופקים בדרך כלל על ידי DHCP, כגון כתובת Default Gateway. כתוצאה מכך, מחשבים בהם אפשרות APIPA זמינה ופעילה יכולים לתקשר רק עם מחשבים שבאותה רשת משנה (subnet) אשר גם לה מזהה רשת 169.254.x.y וכתובת מיסוך 255.255.0.0.

Disabling Automatic Private Addressing

כברירת מחדל מאפיין המיעון האוטומטי - פעיל. אבל, תוכל לבטל אותו באמצעות עורך הרישום על ידי הוספת ערך בשם IPAutoconfigurationEnabled למפתח המשנה HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\Adapter_GUID וקביעת ערכו כאפס (0).

הרשומה IPAutoconfigurationEnabled מקבלת ערך REG_DWORD. כדי לבטל את APIPA הגדר לה ערך 0 (אפס). כדי להפעיל את APIPA הגדר לה ערך 1 (אחד), שזהו מצב ברירת המחדל כאשר IPAutoconfigurationEnabled אינו מופיע ברשומות ה-Registry.

איתור תקלות TCP/IP

Windows 2000 כוללת מספר תוכניות שירות לאיתור תקלות TCP/IP וטיפול בהן. הטבלה הבאה מתארת את תוכניות השירות הכלולות ב- Windows 2000, באמצעותן תוכל לאתר תקלות כאלה ולטפל בהן (יש להקיש את הפקודות האלה במצב Command Prompt):

אפשרות	תיאור
Ping	מוודא תצורה ובוחן חיבורים
Arp	מציג את תוכן מטמון Arp בו ניתן לראות כתובות IP שנקבעו באופן מקומי ככתובות פיסיות.
Ipconfig	מציג את תצורת TCP/IP הנוכחית ואת כל הגדרות כרטיס הרשת
Nbstat	מציג סטטיסטיקה וחיבורים תוך שימוש ב- NetBIOS over TCP/IP
Netstat	מציג סטטיסטיקה וחיבורים של פרוטוקול TCP/IP
Route	מציג או משנה את טבלת הניתוב המקומית
Hostname	מדפיס את שם המארח בו הופעלה הפקודה
Tracert	בוחן את מסלול הניתוב למערכת מרוחקת

בדיקת חיבוריות TCP/IP

Windows 2000 גם מספקת מספר תוכניות שירות שכיחות לניהול ב-TCP/IP. כלים אלה מתוארים בטבלה הבאה:

אפשרות	תיאור
FTP	מאפשר העברת קבצים דו-כיוונית בין מחשב המפעיל את Windows 2000 וכל מחשב TCP/IP מארח, המפעיל FTP. שרת Windows 2000 יכול לשמש כלקוח וכשרת FTP. משמש בעיקר להורדת קבצים מהאינטרנט.
TFTP - **T**rivial **F**ile **T**ransfer **P**rotocol	מאפשר העברת קבצים דו-כיוונית בין מחשב המפעיל את Windows 2000 וכל מחשב TCP/IP מארח המפעיל TFTP.
Telnet	מאפשר הדמיית מסוף למארח TCP/IP המפעיל Telnet. שרת Windows 2000 יכול לשמש כלקוח וכשרת Telnet.
RCP - **R**emote **C**opy **P**rotocol	מעתיק קבצים בין לקוח ומארח התומך ב-RCP (למשל, מחשב Windows 2000 ומארח UNIX).
RSH - **R**emote **Sh**ell	מפעיל פקודות במארח UNIX.
REXEC - **R**emote **Exec**ution	מפעיל הליך (process) במחשב מרוחק.
Finger	מושך נתוני מערכת אודות מחשב מרוחק התומך ב-TCP/IP ובתוכנית השירות Finger.

לאחר הגדרת TCP/IP ואתחול המחשב, עליך להשתמש בתוכניות השירות Ipconfig ו- Ping (אותן מפעילים משורת הפקודה - Command Prompt) כדי לבחון את ההגדרות והחיבורים למארחי TCP/IP אחרים, ולרשתות TCP/IP אחרות. בדיקות שכאלה מאפשרות לך לוודא ש-TCP/IP פועל כשורה.

השימוש ב- Ipconfig

תוכל להיעזר בתוכנית השירות Ipconfig כדי לוודא את הפרמטרים להגדרת TCP/IP במארח. דבר זה יאפשר לך לקבוע אם ההגדרות אותחלו, או אם כבר קיימת כתובת IP זו. השתמש בפקודה עם המתג all/ כדי לבחון את כל נתוני התצורה.

טיפ כדי למנוע מהנתונים המוצגים להיגלל אל מחוץ לחלון שורת הפקודה הקלד את הפקודה **ipconfig /all | more**; כדי לגלול את החלון ולצפות בחלק נוסף של תוכן הפלט, הקש על מקש הרווח. הקלד את הפקודה **ipconfig /all > ipconfig.txt** כדי לכתוב את פלט המסך לקובץ טקסט פשוט בשם ipconfig.txt. אז תוכל לצפות בתוכן הקובץ באמצעות כל עורך ASCII רגיל, כגון Notepad.

הפעלת הפקודה ipconfig /all תציג את התוצאות הבאות:

- אם ההגדרות אותחלו, תציג Ipconfig את כתובת ה-IP ואת ה-Subnet Mask, ואם הוגדר כזה - גם את ה-Default Gateway.
- אם נמצאה כפילות בכתובות IP, מציינת ipconfig את הכתובת, אך כתובת ה-Subnet Mask תהיה 0.0.0.0.
- אם המחשב אינו מסוגל לקבל כתובת IP ממחשב המפעיל שירות DHCP ברשת, תציג Ipconfig את כתובת ה-IP שחולל APIPA (169.254.X.Y).

השימוש ב- Ping

לאחר שווידאת את תצורת TCP/IP השתמש בתוכנית השירות Ping כדי לבחון את החיבוריות. תוכנית השירות Ping היא כלי אבחון באמצעותו תוכל לבדוק תצורות TCP/IP ולאבחן כשלים בחיבורים. השתמש ב- Ping כדי לקבוע אם מארח TCP/IP כלשהו זמין ופעיל. כדי לבחון חיבוריות, השתמש בפקודת Ping במבנה הבא:

ping <IP_Address>

השימוש ב- Ipconfig וב- Ping

ניתן להשתמש בשילוב של הפקודות Ipconfig ו-Ping כדי לוודא תצורת מחשב ולבחון חיבוריות של הנתב (Router). הצעדים הבאים מראים כיצד להשתמש בכלים אלה:

1. הפעל Ipconfig כדי לוודא שתצורת TCP/IP אותחלה.
2. הפעל Ping בתוספת כתובת הלולאה הפנימית (127.0.0.1), כדי לבחון אם TCP/IP מותקן כהלכה וכרוך כראוי לכרטיס מתאם הרשת.
3. הפעל Ping בתוספת מתג כתובת IP של המחשב המקומי, כדי לוודא שלא קיימת כתובת IP זהה לכתובת של המחשב המקומי במקום אחר ברשת.
4. הפעל Ping בתוספת מתג כתובת ה-IP של ה-Default Gateway, כדי לוודא שה-Default Gateway פעיל וכי המחשב יכול לתקשר עם הרשת המקומית.
5. הפעל Ping בתוספת מתג כתובת IP של מארח מרוחק כלשהו, כדי לוודא שהמחשב יכול לתקשר דרך הנתב.

הערה בדרך כלל, אם אתה מבצע את הפקודה Ping מול מארח מרוחק (צעד 5) והתוצאה משביעת רצון ותקינה, צעדים 1 עד 4 תקינים כברירת מחדל. אם הפקודה אינה משיבה תוצאה תקינה, נסה לבצע את הפעולה מול מארח מרוחק אחר, לפני שתשלים את כל תהליך האבחון, מפני שייתכן והמארח המרוחק אינו פעיל באותה נקודה בזמן.

תרגיל 1: הגדרה ובדיקת TCP/IP

בתרגיל זה תשתמש בשתי תוכניות שירות TCP/IP כדי לבחון את תצורת הפרוטוקול במחשב Server01. אחר כך, תגדיר את Server01 לשימוש בכתובת IP קבועה ותבחן את תצורתו החדשה. בשלב הבא תגדיר את Server01 לקבל כתובת IP באופן אוטומטי ואז תבחן את APIPA של Windows 2000. השלם את התרגיל כולו במחשב Server01.

הליך 1: בדיקת תצורת TCP/IP במחשב

בהליך זה תשתמש בשתי תוכניות שירות TCP/IP, Ipconfig ו-Ping, כדי לבחון את התצורה הקבועה שלו:

1. היכנס (Log on) למחשב Server01 בשם משתמש Administrator עם הסיסמה password.
2. פתח את שורת הפקודה (Command Prompt).
3. במחוון הפקודה הקלד את הפקודה **ipconfig /all | more** והקש Enter.

(הקו האנכי שבין המילים all ו- more הוא הקו המקווקו אשר בדרך כלל נמצא על המקש עם סימן הלוכסן האחורי - Backslash, \).

תוכנית השירות Windows 2000 IP Configuration מציגה את תצורת TCP/IP של מתאם/מתאמי הרשת המותקן/ים במחשב שלך.

טיפ בחלון Command Prompt במערכת Windows 2000, ניתן לגלול את תוכן החלון למעלה ולמטה באמצעות סרגל הגלילה האנכי.

4. הקש על מקש הרווח כמה פעמים שנדרש כדי להציג את הכותרת Local Area Connection adapter <adapter type>. השתמש במידע המוצג על המסך כדי להשלים את הערכים החסרים בטבלה הבאה. חלק מהערכים המופיעים בה נוספו באמצעות הליכי הגדרה שביצעת בתרגילים קודמים.

הגדרות Local Area Connection	**ערך**
Host Name	SERVER01
Primary DNS Suffix	microsoft.com
DNS Servers	10.10.10.1
Description	
Physical Address	
DHCP Enabled	No
Subnet Mask	255.0.0.0
Default Gateway	none

5. הקש על מקש הרווח כמה פעמים שנדרש כדי לשוב למחוון הפקודה.

6. כדי לוודא שכתובת ה-IP פועלת כשורה ומוגדרת עבור כרטיס מתאם הרשת שלך, הקלד את הפקודה ping 127.0.0.1 והקש Enter.

כתובת IP זו נקראת LoopBack Address והיא משמשת לדיקת תקינות פעילותה של מחסנית TCP/IP (TCP/IP Stack).

תגובה דומה לזו המתוארת להלן נחשבת לתקינה:

```
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Reply from 127.0.0.1: bytes=32 time<10ms TTL=128
Ping statistics for 127.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 <0% loss>,
Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum =  0ms, Average =  0ms
```

7. מזער את חלון שורת הפקודה. נשתמש בו בהליך מאוחר יותר.

הליך 2: הגדרת TCP/IP לקבלת כתובת IP באופן אוטומטי

בהליך זה תגדיר את TCP/IP, כך שיקבל באופן אוטומטי כתובת IP. אחר כך תבחן את ההגדרות ותוודא ש-APIPA אכן סיפק את נתוני המיעון הנכונים. השלם את ההליך הנוכחי במחשבים Server01 ו-Server02.

1. לחץ על Start, הצבע על Settings ולחץ על Network and Dial-up Connections. חלון Network and Dial-up Connections ייפתח.
2. לחץ על Local Area Connection, פתח את תפריט File ובחר Properties.

   תיבת הדו-שיח Local Area Connection Properties תופיע ובה יוצג כרטיס מתאם הרשת שבשימוש ורכיבי הרשת המשמשים לחיבור הנוכחי.
3. לחץ על Internet Protocol (TCP/IP) ובדוק שתיבת הסימון שמשמאל לרשומת הפרוטוקול מסומנת.
4. לחץ על Properties. תיבת הדו-שיח Internet Protocol (TCP/IP) Properties תופיע.
5. לחץ על לחצן האפשרויות Obtain an IP address automatically.
6. לחץ על לחצן האפשרויות Obtain DNS Server address automatically.
7. לחץ על OK כדי לסגור את תיבת הדו-שיח Internet Protocol (TCP/IP) Properties.
8. לחץ על OK כדי לסגור את תיבת הדו-שיח Local Area Connection Properties.
9. מזער את חלון Network and Dial-up Connections.
10. בשורת הפקודה הקלד **ipconfig /all | more** והקש Enter.
11. הקש על מקש הרווח ככל שיידרש כדי לאתר את הגדרות TCP/IP הנוכחיות עבור Local Area Connection adapter <adapter type>, ורשום אותם בטבלה שלהלן. חלק מהפרטים מולאו עבורך.

הגדרה	ערך
Autoconfiguration Enabled	Yes
IP Address	
Subnet Mask	
DHCP Enabled	Yes
Default Gateway	None - requires manual configuration or DHCP
DNS Servers	None - requires manual configuration or DHCP

שים לב שכתובת ה-IP וה-Subnet-Mask שהוקצו לך על ידי APIPA שונים מאלו שציינת עבור הגדרה ידנית. שים לב גם לכך שכתובת ה-IP מתויגת כעת כ- Autoconfiguration IP Address וכי DHCP פעיל (Enabled). DHCP פעיל מכיון שהגדרת שכתובת ה-IP צריכה להתקבל באופן אוטומטי.

12. הקש על מקש הרווח ככל שיידרש כדי לסיים לגלול את נתוני התצורה.

13. כדי לוודא ש-TCP/IP פועל כשורה וכרוך כהלכה לכרטיס מתאם הרשת שלך, הקלד את הפקודה ping 127.0.0.1 והקש Enter.

אם TCP/IP כרוך לכרטיס מתאם הרשת יוצגו על המסך ארבע תגובות לבדיקת הלולאה הפנימית.

14. צא משורת הפקודה וסגור את חלון Network and Dial-up Connections.

סיכום שיעור

יישומה של Microsoft ל-TCP/IP מאפשר רישות וחיבוריות. חבילת TCP/IP ממופה למודל תפיסתי בן ארבע שכבות: ממשק רשת (Network Interface), אינטרנט (Internet), העברה (Transport) ויישום (Application). כברירת מחדל, מחשבי לקוח הפועלים בסביבת Windows 2000 מקבלים את תצורת ה-TCP/IP באופן אוטומטי משרת DHCP, למרות שמחשבים מסוימים דורשים שתהיה להם כתובת IP קבועה. לכל כרטיס רשת הכרוך לפרוטוקול TCP/IP תוכל להגדיר כתובת IP, Subnet mask ו-Default Gateway. בנוסף, יישום TCP/IP על ידי Windows 2000 תומך גם ב-APIPA, אשר מספק שיוך כתובות IP באופן אוטומטי לתצורות פשוטות של רשתות מבוססות-LAN. APIPA מאפשר הגדרת כתובות IP ללא הצורך בהגדרת כתובת IP קבועה, או התקנת שירות DHCP. Windows 2000 גם כוללת כלי שירות בהם תוכל להיעזר בניסיון לאתר ולטפל בתקלות TCP/IP, ובאמצעותם תוכל לבחון חיבוריות. Ping ו-Ipconfig הן שתי תוכניות שירות שכיחות, ואילו FTP ו-Telnet הם שני שירותי תוכניות שירות.

שיעור 3: DHCP

שירות DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol, הגדרת פרוטוקול מארח דינמי) ב-Windows 2000 מרכז ומנהל את מיקומי נתוני תצורות TCP/IP, על ידי הקצאת כתובות IP ונתוני תצורת TCP/IP אחרת באופן אוטומטי למחשבים המוגדרים כלקוחות DHCP. יישום שירות DHCP יכול למנוע תקלות רבות הקשורות להגדרת TCP/IP באופן ידני. שיעור זה דן במיומנויות הנדרשות ומספק מידע אודות התקנה והגדרה של שירות DHCP. בנוסף הוא גם דן בתהליך החכירה (Lease) של DHCP.

לאחר שיעור זה, תוכל

- להתקין את שירות DHCP.
- ליצור מרחב (Scope) עבור שירות DHCP **ולהגדיר טווח כתובות** (Address Range) **ושמירת כתובות** (Address Reservation) **עבור הגדרות** Scope.
- לגבות **ו**לשחזר מסד נתוני DHCP.

זמן לימוד משוער: 70 דקות

מבוא ל-DHCP

DHCP הוא תקן TCP/IP שנועד לפשט את נושא ניהול תצורת TCP/IP. DHCP הוא הרחבה של פרוטוקול Bootstrap (BOOTP), המבוסס על UDP/IP (**U**ser **D**atagram **P**rotocol/**I**nternet **P**rotocol). BOOTP מאפשר למארח מאתחל להגדיר את עצמו באופן דינמי.

בכל פעם שלקוח DHCP מאותחל הוא מבקש נתוני מיעון משרת DHCP. נתוני המיעון כוללים:

- כתובת IP.
- subnet mask.
- ערכים אפשריים, כגון Default Gateway, כתובת שרת DNS או שרת WINS.

כאשר שרת DHCP מקבל בקשה לכתובת IP, הוא בוחר את נתוני המיעון ממאגר כתובות המוגדרות במסד הנתונים שלו ומציע את נתוני המיעון ללקוח DHCP. אם הלקוח מקבל את ההצעה, שרת ה-DHCP מחכיר (Lease) לו את נתוני מיעון ה-IP למשך זמן קצוב מראש.

הגדרת TCP/IP אוטומטית או ידנית

כדי להבין מדוע שירות DHCP מייעל את הגדרת TCP/IP בלקוחות, השווה את שיטת ההגדרה הידנית לעומת זו הנעזרת בשירותי DHCP, כפי שמוצג בטבלה הבאה.

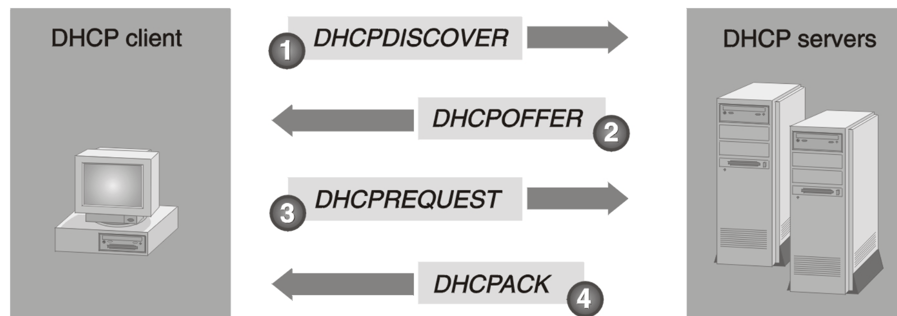
הגדרה ידנית של TCP/IP	הגדרת TCP/IP באמצעות DHCP
משתמש יכול לבחור באקראי כתובת IP, במקום לקבל ממנהל הרשת כתובת חוקית ופנויה. השימוש בכתובת IP שגויה יכול לגרום לתקלות ברשת ומקור התקלה עלול להיות קשה לזיהוי.	משתמשים כבר אינם צריכים להשיג נתוני מיעון IP ממנהל הרשת כדי להגדיר את TCP/IP אצלם. שירות DHCP מספק את כל נתוני התצורה הדרושים לכל לקוחות DHCP.
הקלדה של כתובת IP, Subnet Mask או Default Gateway, עלולה לגרור אחריה תקלות: החל בתקלות תקשורת, אם Default Gateway או Subnet Mask אינה נכונה, וכלה בתקלות המשויכות לכפילויות בכתובות IP.	נתוני מיעון IP חוקיים מבטיחים הגדרה נכונה, דבר שימנע את רוב בעיות הרשת הקשות לאיתור.
תקורת ניהול הרשת עולה, אם עליך להעביר מחשבים בין רשתות משניות לעיתים קרובות. לדוגמה, עליך לשנות את כתובת ה-IP ואת Default Gateway כדי שלקוח יוכל לתקשר עם מיקום חדש.	כאשר עומדים לרשותך שרתים המפעילים את שירות DHCP בכל רשת משנה, יורדת תקורת הניהול המשויכת להגדרה ידנית של כתובות IP, Subnet Mask ו-Default Gateway, כאשר אתה מעביר מחשבים בין רשתות משניות שונות. שים לב ששרת DHCP יחיד יכול לתמוך בשיוך כתובות IP עבור מספר רשתות.

DHCP Lease Process

שירות DHCP משייך נתוני מיעון IP למחשבי לקוח. שיוך נתוני המיעון נקרא **חכירת DHCP** (DHCP Lease). תהליך חכירת DHCP מתרחש בעת התרחשות אחד מהאירועים הבאים:

- TCP/IP מאותחל בפעם הראשונה בלקוח DHCP.
- לקוח מבקש כתובת IP מסוימת, אך בקשתו נדחית, ייתכן שכתוצאה מכך ששרת DHCP סיים את תקופת החכירה.
- לקוח חכר בעבר כתובת IP, אך שחרר אותה וכעת מבקש כתובת חדשה. חכירת DHCP יכולה להיות משוחררת באופן ידני משורת הפקודה (Command prompt) על ידי הקלדת הפקודה **ipconfig /release**.

DHCP מבצע תהליך בן ארבעה שלבים לחכירת נתוני תצורת רשת ללקוחותיו, למשך זמן מוקצב: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST ו-DHCPACK (ראה תרשים 9.5).



תרשים 9.5 תהליך החכירה של DHCP.

DHCPDISCOVER

הצעד הראשון בתהליך החכירה של DHCP הוא DHCPDISCOVER. כדי להתחיל את תהליך החכירה, מאתחל הלקוח גירסה מוגבלת של TCP/IP ומשדר הודעת DHCPDISCOVER ובה שאילתה היכן נמצא שרת DHCP, ובקשה לנתוני מיעון IP (IP Addressing Information). מכיון שהלקוח אינו יודע את כתובת ה-IP של שרת DHCP הוא משתמש בכתובת 0.0.0.0 ככתובת המקור ובכתובת 255.255.255.255 ככתובת היעד. הודעת DHCPDISCOVER מכילה את כתובת החומרה ואת שם מחשב הלקוח, כך ששרתי ה-DHCP מסוגלים לקבוע איזה לקוח שלח את הבקשה.

DHCPOFFER

הצעד השני בתהליך החכירה הוא DHCPOFFER. כל שרתי DHCP המקבלים את בקשת החכירה והכוללים תצורות לקוח חוקיות, משדרים הודעת DHCPOFFER אשר כוללת את הנתונים הבאים:

❖ כתובת החומרה של הלקוח.

❖ הצעה לכתובת IP.

❖ Subnet Mask.

❖ אורך חיי חוזה החכירה (כמה זמן תישאר הכתובת ברשות המחשב).

❖ מזהה שרת (כתובת ה-IP של שרת ה-DHCP המציע).

שרת ה-DHCP שולח הודעה (broadcast) מכיון שללקוח עדיין אין כתובת IP. לקוח DHCP בוחר כתובת IP מההצעה הראשונה שהוא מקבל. שרת DHCP, המנפק את כתובת ה-IP, שומר אותה באופן שלא ניתן יהיה להציעה ללקוח DHCP אחר.

DHCPREQUEST

הצעד השלישי בתהליך החכירה מתבצע לאחר שהלקוח מקבל הודעת Broadcast מסוג DHCPOFFER משרת DHCP אחד לפחות, ובוחר לעצמו כתובת IP. הלקוח משדר הודעת DHCPREQUEST לכל שרתי DHCP, פעולה שמסמנת שהוא כבר הסכים להצעה. הודעת DHCPREQUEST כוללת את מזהה השרת (כתובת ה-IP) של השרת שהצעתו התקבלה. כל יתר שרתי ה-DHCP מושכים את הצעותיהם חזרה, ומשחררים את כתובות ה-IP לבקשת החכירה הבאה.

DHCPACK

הצעד האחרון בתהליך חכירה מוצלח מתרחש כאשר שרת ה-DHCP, שלהצעתו הסכים הלקוח, משדר ללקוח הודעת אישור על הצלחת התהליך. זו הודעת DHCPACK, והיא מכילה חוזה חכירה חוקי לכתובת IP וייתכן שגם נתוני תצורה נוספים.

כשלקוח DHCP מקבל את האישור, TCP/IP מאותחל לחלוטין והלקוח נחשב לקוח DHCP כרוך (Bound DHCP Client) מן המניין. כעת הוא יכול להשתמש ב-TCP/IP לצורך התקשרויות רשת.

DHCPNACK

אם שלב DHCPREQUEST לא הסתיים כהלכה, משדר שרת ה-DHCP הודעת אי-אישור (DHCPNACK). שרת DHCP ישדר הודעת DHCPNACK באחד מהמקרים הבאים :

- ❖ הלקוח מנסה לחכור את כתובת ה-IP הקודמת שלו, וכתובת זו כבר אינה זמינה.
- ❖ כתובת ה-IP אינה חוקית, מכיון שמחשב הלקוח הועבר ל-Subnet Mask שונה.

כאשר מקבל הלקוח הודעת DHCPNACK הוא מתחיל את תהליך הבקשה לחכירה מחדש.

הערה אם במחשב מותקנים כמה כרטיסי מתאם רשת הכרוכים (Bound) ל-TCP/IP, תהליך DHCP מתבצע באופן נפרד עבור כל אחד מהכרטיסים. שירות DHCP מעניק כתובת IP ייחודית וחוקית לכל כרטיס מותקן הכרוך עם TCP/IP.

IP Lease Renewal and Release

כל לקוחות DHCP מנסים לחדש את חוזה החכירה שלהם כאשר עוברים 50% מאורך חיי החוזה. כדי לחדש חוזה חכירה, שולח לקוח ה-DHCP הודעת DHCPREQUEST ישירות לשרת ה-DHCP ממנו חכר את הכתובת הנוכחית. אם שרת ה-DHCP זמין, הוא מחדש את החוזה ושולח ללקוח הודעת DHCPACK ובה משך זמן חדש עד לפקיעת החוזה ונתוני תצורה מעודכנים, אם קיימים. הלקוח מעדכן את תצורתו כאשר הוא מקבל את הודעת האישור.

הערה בכל פעם שלקוח DHCP מאותחל הוא מנסה לחכור את אותה כתובת IP משרת ה-DHCP המקורי. אם בקשת החכירה אינה מצליחה ועדיין נשאר זמן עד למועד פקיעת החוזה, ממשיך לקוח ה-DHCP להשתמש בכתובת ה-IP הקיימת, עד לניסיון הבא לחידוש החוזה.

אם לקוח DHCP אינו מצליח לחדש את חוזה החכירה עם שרת ה-DHCP המקורי כאשר עברו 50% ממועד פקיעת החוזה, ממתין הלקוח עד שיעברו 87.5% מאורך חיי החוזה ומשדר הודעת DHCPREQUEST כדי ליצור קשר עם שרת DHCP זמין כלשהו. כל שרת DHCP יכול לענות בהודעת DHCPACK (מאשר את חידוש החוזה) או DHCPNACK (הודעת אי-אישור) המכריחה את הלקוח להשיג חוזה חדש עבור כתובת IP שונה.

אם תוקף החוזה פג, או שהתקבלה הודעת DHCPNACK, חייב הלקוח להפסיק את השימוש בכתובת ה-IP באופן מיידי. מאותו רגע מתחיל לקוח ה-DHCP את תהליך החכירה מראשיתו, בניסיון לקבל חוזה חכירה לכתובת IP חדשה.

הערה הוויתור על כתובת IP נעשה מצד הלקוח. ה-DHCP לא שולח פקודה לשיחרור הכתובת.

השימוש ב- Ipconfig לחידוש חוזה חכירה

השתמש בפקודה Ipconfig /Renew למשלוח הודעת DHCPREQUEST לשרת DHCP, כדי לקבל אפשרויות מעודכנות ואת משך חוזה החכירה. אם שרת ה-DHCP אינו זמין, ממשיך הלקוח להשתמש באותן אפשרויות תצורת DHCP שסופקו לו.

השימוש ב- Ipconfig לשחרור חוזה חכירה

השתמש בפקודה Ipconfig /release כדי לגרום ללקוח DHCP לשלוח הודעת DHCPRELEASE לשרת DHCP, וכדי לשחרר את חוזה החכירה שלו. פעולה זו יעילה כאשר אתה מעביר לקוח לרשת אחרת, והלקוח לא יצטרך את חוזה החכירה הקודם שלו. תקשורת TCP/IP עם הלקוח מפסיקה מייד לאחר הפעלת הפקודה.

לקוחות DHCP אינם יוצרים הודעות DHCPRELEASE כאשר הם "יורדים". ללקוח DHCP יש סיכוי טוב יותר לקבל את אותה כתובת IP בעת האתחול אם הוא אינו שולח הודעת DHCPRELEASE, אך אם לקוח נשאר כבוי למשך זמן ארוך מאורך חיי חוזה החכירה שלו (והחוזה עדיין לא חודש), יכול שרת ה-DHCP להקצות את כתובת ה-IP של לקוח זה ללקוח אחר, לאחר שפג תוקף החוזה.

הערה למידע נוסף אודות DHCP **ואודות יישום** DHCP, פנה לתקליטור המצורף לספר זה (\chapt09\articles\dhcp2000.doc).

התקנת שירות DHCP והגדרתו

כדי ליישם DHCP, עליך להתקין את שירות DHCP ולהגדירו לפחות במחשב אחד, הפועל בסביבת Windows 2000 Server ברשת TCP/IP. המחשב יכול להיות מוגדר כ-Domain Controller, או כ-Stand-alone Server. בנוסף, כדי ששירות DHCP יתפקד כהלכה, עליך להגדיר באופן ידני את תצורת TCP/IP בשרת ולהגדיר את הלקוחות לקבלת תצורת כתובות באופן דינמי.

דרישות שרת להפעלת שירות DHCP

שרת DHCP חייב להיות מחשב בו מותקן שרת Windows 2000, המוגדר כדלקמן:

- כתובת IP קבועה, Subnet Mask, Default Gateway (אם נדרש) ופרמטרים אחרים של TCP/IP. שרת DHCP אינו יכול להיות לקוח DHCP.
- שירות DHCP.
- DHCP Scope פעיל. scope הוא טווח (range) כתובות IP אשר זמינות לחכירה או לשיוך ללקוחות. מרגע שנוצר תחום ההגדרה, הוא חייב להיות פעיל.
- הרשאה (Authorization). לשרת DHCP חייבת להיות הרשאה בשירותי Active Directory.

דרישות לקוח DHCP

לקוח DHCP צריך להיות מחשב המוגדר לצורך זה, ואשר פועל בסביבת אחת ממערכות ההפעלה התואמות הבאות:

- ❖ Windows 2000.
- ❖ Windows NT Server גירסה 3.51 ומעלה.
- ❖ Windows NT Workstation גירסה 3.51 ומעלה.
- ❖ Windows 98.
- ❖ Windows 95.
- ❖ Windows for Workgroups 3.11 (המפעילה Microsoft TCP/IP-32).
- ❖ Microsoft Network Client עבור Microsoft MS-DOS (עם מנהלי התקן TCP/IP במצב אמיתי).
- ❖ LAN manager גירסה 2.2c עבור MS-DOS (LAN manager גירסה 2.2c עבור OS/2 אינו נתמך).

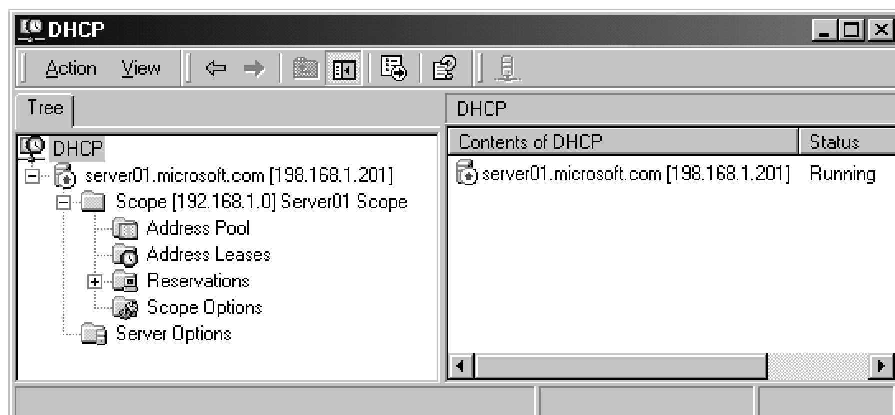
התקנת שירות DHCP

הצעד הראשון לקראת יישום DHCP ברשת הוא התקנת שירות DHCP. לפני שתתקין שירות זה, עליך לקבוע למחשב המיועד כתובת IP קבועה, Subnet Mask ו-Default Gateway עבור כרטיס הרשת הכרוך עם TCP/IP.

כדי להתקין את השירות, השתמש ביישומון Add/Remove Programs שב-Control Panel. שירות DHCP מופעל באופן אוטומטי בעת ההתקנה, וחייב להיות פעיל כדי לתקשר עם לקוחות DHCP.

תוסף התוכנה (Snap-in) של DHCP

תוכל להיעזר בתוסף התוכנה של DHCP, כפי שמוצג בתרשים *9.6*, לביצוען של כל משימות ההגדרה והניהול של DHCP. תוסף התוכנה של DHCP מאפשר גישה לנתונים מפורטים של תחומי ההגדרה (Scope) והאפשרויות של DHCP. בנוסף, הוא מאפשר לך ליצור ולשנות תחומי הגדרה, לצפות בחוזי חכירה של כתובות, ליצור ולשנות שמירות עבור לקוחות וגם להגדיר אפשרויות שרת, Scope, הגדרות ושמירה עבור לקוחות.



תרשים 9.6 תוסף התוכנה של DHCP.

תוכל לגשת לתוסף התוכנה (Snap-in) של DHCP כ-MMC Console בודדת, או באמצעות תוסף תוכנה אחר בשם Computer Management. תוסף התוכנה של DHCP יכול להיות מותקן באמצעות הפעלת Adminpak.msi או על ידי התקנת שירות DHCP. לפני התקנת שירות DHCP יוכל לשמש תוסף התוכנה של DHCP לניהול שרתים מרוחקים המפעילים את שירות DHCP.

יצירת DHCP Scope

לאחר שהתקנת את שירות DHCP והוא פעיל, הצעד הבא הוא ליצור **מרחב כתובות** (Address Scope). המרחב (Scope) חייב להיות מוגדר לפני ששרת DHCP יוכל להחכיר כתובות IP ללקוחות DHCP. מרחב הוא קבוצת כתובות IP חוקיות, אותן יכולים לקוחות DHCP לחכור.

בעת יצירת מרחב DHCP רצוי להתחשב בקווים המנחים הבאים:

- עליך ליצור לפחות Scope אחד לכל שרת DHCP.
- יש למנוע מצב בו מופיעות במרחב הכתובות כתובות IP קבועות.
- ניתן להגדיר מספר Scopes בשרת DHCP אחד, כדי לרכז את ניהולם ולהגדיר כתובות IP ייחודיות ל-Subnet Mask. ניתן להגדיר רק מרחב אחד ל-Subnet Mask מסוימת.
- שרתי DHCP אינם יכולים לשתף את נתוני ה-scope. כתוצאה מכך, כשאתה יוצר scopes במספר שרתי DHCP, ודא שאינך מגדיר את אותן כתובות IP בשני שרתים, כדי למנוע כפילות כתובות IP.

כדי ליצור scope, היעזר בתוסף התוכנה של DHCP. הטבלה הבאה מתארת כמה מהפרמטרים אותם עליך לקבוע כשאתה יוצר מרחב חדש:

פרמטר	תיאור
Name	שם המרחב (Scope)
Description	תיאור אופציונלי של המרחב
Start IP Address	כתובת ה-IP הראשונה בטווח הכתובות, שיכולה להיות מוחכרת ממרחב זה ללקוח DHCP.
End IP Address	כתובת ה-IP האחרונה בטווח הכתובות, שיכולה להיות מוחכרת ממרחב זה ללקוח DHCP.
Subnet Mask	Subnet Mask המוגדרת ללקוחות DHCP. ניתן להגדיר Subnet Mask לפי מספר הסיביות, או במבנה מסכת קלאסי.
Start IP Address	כתובת ה-IP הראשונה ברשימה שמיועדת להוצאה אל מחוץ לקבוצת הכתובות. כתובות אלו לא יחולקו ללקוחות DHCP. השתמש במאפיין זה אם יש לך כתובות קבועות המוגדרות במחשבים שאינם לקוחות DHCP (הגדרה זו היא אופציונלית).
End IP Address	כתובת ה-IP האחרונה ברשימה שמיועדת להוצאה אל מחוץ לקבוצת הכתובות. כתובות אלו לא יחולקו ללקוחות DHCP. השתמש במאפיין זה אם יש לך כתובות קבועות המוגדרות במחשבים שאינם לקוחות DHCP (הגדרה זו היא אופציונלית).
Lease Duration	מספר הימים, השעות והדקות, בהן חוזה החכירה של לקוח DHCP תקף, לפני שיהיה צורך לחדשו.

לאחר שיצרת את המרחב (Scope), עליך להפעיל אותו כדי להפוך אותו לזמין למשימות החכרה שעליו לבצע. כדי להפעיל (Activate) את המרחב - בחר בו ואז, מתפריט Action בחר Activate.

הערה כדי להגדיר כתובת Subnet Mask חדשה, לאחר אישור ההגדרות, עליך ליצור Scope חדש ולמחוק את הקיים (במידה וטווחי הכתובות מתנגשים).

הגדרת DHCP Scope

לאחר שיצרת את DHCP Scope, תוכל להגדיר אפשרויות שונות עבור לקוחות DHCP. קיימות שלוש רמות של אפשרויות מרחב: Server, Scope, Client.

Server Options

אפשרויות השרת זמינות לכל לקוחות DHCP. היעזר באפשרויות השרת, כאשר כל הלקוחות בכל רשתות המשנה דורשים את אותם נתוני הגדרה. לדוגמה, ייתכן שתרצה להגדיר שכל הלקוחות ישתמשו באותו שרת WINS. אפשרויות השרת מוגדרות תמיד, אלא אם מוגדרות Scope Options או Client Options. להגדרת אפשרויות **שרת**, לחץ על Action, הצבע על Server Options ובחר Configure Options.

Scope Options

אפשרויות המרחב זמינות רק עבור לקוחות החוכרים כתובות ממרחב מסוים. לדוגמה, אם יש לך מרחב (Scope) שונה עבור כל רשת משנה (Subnet), תוכל להגדיר כתובת Default Gateway ייחודית ושונה לכל רשת משנה. הגדרות **מרחב** (Scope) רומסות את הגדרות השרת. כדי להגדיר אפשרויות מרחב, בחר ב-Scope המבוקש, פתח את תפריט Action ובחר Configure Options.

Client Options

אפשרויות לקוח זמינות עבור לקוחות מסוימים, להם שמורים חוזי חכירה לכתובות מסוימות (Reserved DHCP address leases). אפשרויות לקוח תמיד מתבצעות לפני אפשרויות שרת או מרחב. כדי להגדיר אפשרויות לקוח, בחר את רשומת השמירה (Reservation) המיוחדת ללקוח, פתח את תפריט Action ובחר Configure Options.

הגדרת DHCP Options

הטבלה הבאה מתארת חלק מהאפשרויות הזמינות בעת הגדרת DHCP Server, Scope או Client Reservation. תיבות הדו-שיח Properties של שרת DHCP, מרחב (Scope) ושמירה עבור לקוח (Client Reservation), כוללות את כל הרכיבים הנתמכים על ידי Microsoft DHCP.

אפשרות	תיאור
003 Router	כתובת IP של נתב (Router), כגון כתובת Default Gateway. Default Gateway המוגדר בלקוח באופן מקומי מקבל קדימות על פני האפשרות המוגדרת ב-DHCP. כדי לוודא שנתוני הנתב נשלחים למחשב הלקוח, ודא שתיבת הטקסט Default gateway במחשב הלקוח נשארה ריקה (ראה תרשים 9.4).
006 DNS Servers	כתובת IP של שרת DNS. שרת DNS המוגדר בלקוח באופן מקומי מקבל קדימות גבוהה על פני האפשרות המוגדרת ב-DHCP. ודא שלחצן האפשרויות Obtain DNS server address automatically מסומן במחשב הלקוח (ראה תרשים 9.4).

אפשרות	תיאור
015 DNS Domain Name	שם DNS Domain בו ישתמש הלקוח לתרגום שם מארח.
044 WINS/NBNS Servers	כתובת IP של שרת WINS/NBNS זמין ללקוחות. אם כתובת שרת WINS מוגדרת באופן ידני בלקוח, ההגדרה הידנית מקבלת קדימות על פני ערכים אחרים המוגדרים לאפשרות זו.
046 WINS/NBT Node Type	קביעת סוג האמצעי לתרגום השם עבור NetBIOS over TCP/IP, בו ישתמש הלקוח. האפשרויות הן: **1** = צומת B (Broadcast), **2** = צומת P (Peer), **4** = צומת M (Mixed), ו- **8** = צומת H (Hybrid).
047 NetBIOS Scope ID	מזהה מרחב מקומי עבור NetBIOS over TCP/IP. NetBIOS over TCP/IP מתקשר רק עם מארחי NetBIOS שיש להם אותו מזהה מרחב.

הטבלה הבאה מתארת את סוגי הערכים הניתנים לשימוש בעת הגדרת אפשרויות DHCP.

סוג ערך	תיאור
IP Address	כתובת IP של השרת, לדוגמה 003 Routers
Long	ערך מספרי בן **32** סיביות, לדוגמה 035 ARP Cache Timeout.
String Value	מחרוזת תווים, לדוגמה 015 Domain Name.
Word	ערך מספרי בן **16** סיביות עבור גדלים מוחלטים של בלוקים, לדוגמה 022 Max DG Reassembly Size.
Byte	ערך מספרי המכיל בית (Byte) בודד, לדוגמה 046 WINS/NBT Node Type
Binary	ערך בינארי, לדוגמה 043 Vendor-specific information.

Client Reservation

ללקוחות DHCP מסוימים חשוב כי תוקצה להם כתובת IP קבועה, כאשר חוזה החכירה שלהם מסתיים. לדוגמה, מחשבי לקוח המפעילים שירותי שרת TCP/IP, עשויים להסתמך על תצורת כתובת IP קבועה, כדי שיזוהו נכון על ידי לקוחות אחרים ברשת. תוכל להגדיר את שירותי DHCP כך שתמיד יקצו את אותה כתובת IP ללקוחות המפעילים שירותי שרתים (Server Services). פעולה זו נקראת **שמירה עבור לקוח** (Client Reservation), והיא נוצרת באמצעות תיבת הדו-שיח New Reservation המוצגת בתרשים 9.7.

תרשים 9.7 השימוש בתיבת הדו-שיח New Reservation להוספת הגדרת שמירה עבור לקוח.

לקוחות המשתמשים באמצעי סטטי לתרגום שמות, עשויים לדרוש משרתים קריטיים שישמרו על תצורת כתובת IP קבועה. לדוגמה, אם שרת ששם המארח שלו SRV187 נמצא ברשת המכילה מחשבי לקוח המבצעים את נושא תרגום השמות באמצעות קובץ HOSTS או LMHOSTS סטטי והשרת מוגדר כלקוח DHCP, יש להגדיר לשרת SRV187 נתוני IP קבועים באמצעות Reservation Client ברשת DHCP, באותה רשת. הגדרה זו מבטיחה כי SRV187 תמיד יחכיר את אותה כתובת IP עבורו והלקוחות יוכלו להשתמש בנתוני מיפוי שם-כתובת IP (Name-to-IP-address mapping) סטטיים עבור תרגום השמות. בקובץ LMHOSTS ישתמשו לקוחות הזקוקים לתרגום שמות NetBIOS וברשת שלהם לא פועל שרת WINS ואילו בקובץ HOSTS ישתמשו לקוחות הזקוקים לתרגום שם מארח (HOST) וברשת שלהם לא פועל שרת DNS.

כדי להגדיר שמירה עבור לקוח בחר במרחב הכתובות (Scope), פתח את תפריט Action, בחר Reservations, ואז בחר New Reservation. כשאתה מגדיר שמירה עבור לקוח, ודא כי אתה מקליד כתובת IP נכונה וכתובת MAC מדויקת. אם תקליד ערך MAC לא נכון לא תהיה התאמה בינו ובין הערך שנשלח על ידי לקוח DHCP, ושירות DHCP יקצה ללקוח כתובת IP זמינה כלשהי מטווח הכתובות, במקום את הכתובת השמורה במיוחד עבורו. אם אתה מחליף את כרטיס מתאם הרשת של מחשב המקבל שירותי שמירת כתובת, ודא כי אתה מגדיר מחדש את השמירה, כך שתתאים לכתובת MAC החדשה של הלקוח.

Authorizing the DHCP Server

לפני ששרת DHCP יוכל להקצות כתובות IP, הוא חייב להיות מורשה על ידי שירותי Active Directory. אישור (Authorization) הוא אמצעי אבטחה, המבטיח שרק שרתי DHCP מורשים יפעלו ברשת שלך. כדי לאשר DHCP Server בחר ב-Domain בעץ תוסף התוכנה של DHCP ומתפריט Action בחר Authorize.

תרגיל 2: התקנה והגדרה של שירות DHCP

בתרגיל זה תתקין ותגדיר את שירות DHCP בשרת Server01. תיצור scope ותגדיר טווח קטן של כתובות עבורו. כפי שעשית בתרגיל הקודם, ודא כי Server01 נמצא ברשת נפרדת, כך שלא יתנגש עם כתובות IP ברשת גדולה יותר. בצע חלק מההליכים בשרת Server01 וחלק אחר בשרת Server02, כפי שיפורט בהמשך.

הליך 1: הגדרה מחדש של TCP/IP לשימוש בכתובת IP קבועה בשרת Server01

בהליך זה תגדיר את Server01 להשתמש בכתובת IP קבועה; זוהי דרישה מקדימה להתקנת שירות DHCP.

1. היכנס לשרת Server01 בשם משתמש Administartor ועם הסיסמה password.
2. לחץ Start, הצבע על Settings ולחץ על Network and Dial-up connections. חלון Network and Dial-up connections ייפתח.
3. לחץ על Local Area Connection, פתח את תפריט File ובחר Properties.

   תיבת הדו-שיח Local Area Connection Properties תיפתח, ותציג את כרטיס הרשת המשמש את רכיבי הרשת לחיבור זה.
4. לחץ על Internet Protocol (TCP/IP), וודא כי תיבת הסימון ליד רשומה זו מסומנת.
5. לחץ Properties. תיבת הדו-שיח Internet Protocol (TCP/IP) Properties תיפתח.
6. לחץ על לחצן האפשרויות Use the following IP address.
7. בתיבה IP Address הקלד **192.168.1.201**, הקש Tab וודא כי בתיבה Subnet mask מופיע 255.255.255.0.
8. לחץ OK. תיבת הודעה שכותרתה Microsoft TCP/IP תופיע ותציין כי רשימת שרתי DNS ריקה, וכי ייעשה שימוש בכתובת IP מקומית מכיון שבמחשב זה מותקן DNS.
9. לחץ OK, כדי לאשר את ההודעה.
10. לחץ OK, כדי לסגור את תיבת הדו-שיח Local Area Connection Properties.
11. מזער את חלון Network and Dial-up connections.

הליך 2: קביעת כתובתו הפיסית של מחשב

בהליך זה תקבע את כתובתו הפיסית של השרת Server02. תשתמש בכתובת פיסית זו (כתובת MAC) בהליך מאוחר יותר כדי לקבוע שמירה עבור לקוח (DHCP Reservation).

1. ודא כי Server02 מחובר לאותה רשת נפרדת אליה מחובר Server01 ואז היכנס אליו בשם משתמש Administartor ועם הסיסמה password.
2. פתח חלון שורת פקודה (Command Prompt) והקלד את הפקודה **ipconfig /all | more**, כדי לקבוע את כתובתו הפיסית (MAC Address) של כרטיס מתאם הרשת Local Area Network adapter <adapter type> בשרת Server02.

הערה אם Server02 הוגדר עם כתובת IP חוקית, אליה יכול Server01 להגיע, תוכל לבצע ping לכתובת IP מתוך Server01. הקלד **arp -a** והקש Enter, כדי לקבוע משרת Server01 את כתובתו הפיסית של כרטיס מתאם הרשת בשרת Server02.

---

3. רשום את הכתובת הפיסית של Server02 בשורה למטה.

   הכתובת הפיסית היא כתובת החומרה או כתובת MAC. זוהי הכתובת הצרובה באופן קבוע לכרטיס מתאם הרשת שלך והיא אמורה להיראות דומה לדוגמה הבאה: 00-50-04-B4-3A-23.

   כתובת MAC:

4. מזער את חלון שורת הפקודה בשרת Server02.

הליך 3: התקנת שירות DHCP

בהליך זה תתקין את שירות DHCP בשרת Server01.

1. ב- Server01, לחץ Start, הצבע על Programs והצבע על Administrative Tools. שים לב ש-DHCP מופיע ברשימת כלי הניהול. תוסף התוכנה של DHCP כבר קיים, מכיון שהתקנת את Adminpak.msi באחד התרגילים הקודמים. זהו רק תוסף התוכנה של DHCP. שירות DHCP עדיין אינו מותקן בשרת Server01.
2. לחץ Start, הצבע על Settings ולחץ על Control Panel.
3. לחץ לחיצה כפולה על הסמל Add/Remove Programs.

   חלון Add/Remove Programs יופיע.

4. לחץ על Add/Remove Windows Components במסגרת השמאלית.

   האשף Windows Components יופיע.

5. בתיבה Components לחץ על Networking Services, אבל היזהר שלא לשנות את מצבה של תיבת הסימון שמשמאל לאפשרות זו.

הערה תיבת הסימון ליד Networking Services כבר מסומנת, מכיון שחלק משירותי הרישות כבר הותקנו בשרת Server01.

---

6. לחץ על Details. תיבת הדו-שיח Networking Services תופיע.

   בתיבה Subcomponents of Networking Services סמן את תיבת הסימון ליד Dynamic Host Configuration Protocol (DHCP).

7. לחץ על OK. החלון Windows Components יופיע.

8. לחץ Next. המסך Configuring Components מציג את שינויי ההגדרות שביקשת. תיבת הודעה File Copy מופיעה כאשר מועתקים קבצי DHCP לתיקיות מערכת ההפעלה. כעת מופיע חלון האשף Completing the Windows Components Wizard.

9. לחץ Finish.

10. סגור את חלון Add/Remove Programs.

11. סגור את חלון Control Panel.

הליך 4: יצירה והגדרה של DHCP Scope

בהליך זה תיצור ותגדיר DHCP Scope בשרת Server01.

1. לחץ Start, הצבע על Programs, הצבע על Administrative Tools ובחר DHCP.

   תוסף התוכנה של DHCP יופיע.

2. הגדל את חלון DHCP תוסף התוכנה לגודלו המירבי.

3. בחלון Tree, לחץ לחיצה כפולה על [Server01.microsoft.com[192.168.1.201.

   בחלונית הפרטים תופיע ההודעה Configure the DHCP Server.

4. קרא את ההודעה המופיעה בחלונית הפרטים.

5. פתח את תפריט Action ולחץ New Scope. האשף New Scope יופיע.

6. לחץ Next. יופיע המסך Scope Name.

7. בתיבת הטקסט Name, הקלד **Server01 Scope**.

8. בתיבת הטקסט Description הקלד **Training network**, ולחץ על Next.

   יופיע המסך IP Address Range.

9. בתיבה Start הקלד **192.168.1.70** ובתיבה End הקלד **192.168.1.90**.

שים לב ש-Subnet Mask מוגדרת כברירת מחדל לכתובת תקנית של מחלקה C (Class C Address), 255.255.255.0, וכי 24 סיביות מאופשרות; כל הסיביות בשלושת האוקטטים הראשונים בבינארית מוגדרים לערך 1.

10. לחץ Next. יופיע המסך Add Exclusions.

11. בתיבה Start Address הקלד **192.168.1.76**.

12. בתיבה End Address הקלד **192.168.1.80**.

13. לחץ Add. שים לב שהכתובות 192.168.1.76 עד 192.168.1.80 מופיעות בתיבה Excluded Addresses.

14. לחץ Next. יופיע החלון Lease Duration. קרא את המידע בדף זה, ושים לב שברירת המחדל עבור אורך חיי חוזה החכירה היא שמונה ימים.

15. לחץ Next כדי לאשר את ברירת המחדל של אורך חיי החוזה.

יופיע המסך Configure DHCP Options ובו תישאל האם ברצונך להגדיר את אפשרויות DHCP השכיחות ביותר כעת.

16. לחץ על לחצן האפשרויות No, I will configure these options later (לא, אגדיר אפשרויות אלה מאוחר יותר), ולחץ Next.

יופיע מסך Completing the new scope wizard.

17. קרא את ההוראות במסך זה ולחץ Finish בסיום. בחלון DHCP Manager מופיע סמל המייצג את ה-scope החדש שזה עתה יצרת.

החץ האדום המורה כלפי מטה מציין ש-scope זה עדיין אינו פעיל. אתה תהפוך אותו לפעיל בהליך מאוחר יותר.

הליך 5: הוספת שמירה עבור לקוח ב-DHCP Scope

בהליך זה תיעזר בכתובת הפיסית של Server02, כפי שרשמת לפניך בהליך 2, כדי להוסיף ל- DHCP scope שמירה עבור לקוח (Reservation).

1. בתוסף התוכנה של DHCP הפועל בשרת Server01, לחץ על Server01 Scope [192.168.1.0] Scope שבחלון Tree. תוכן המרחב (Scope) יופיע בחלונית הפרטים.
2. בחלון Tree, לחץ על Reservations וקרא את ההודעה המופיעה בחלונית הפרטים.
3. פתח את תפריט Action ולחץ על New Reservation.

   תיבת הדו-שיח New Reservation תיפתח.
4. בתיבת הטקסט Reservation Name הקלד **Server02**.
5. בתיבה IP Address, שים לב ששלושת האוקטטים הראשונים כבר נרשמו עבורך. באוקטט הרביעי הקלד 76. התיבה אמורה להכיל כעת את הכתובת 192.168.1.76.
6. בתיבה MAC Address הקלד את הכתובת הפיסית אותה רשמת בהליך 2. אל תקליד את המקפים.

   לדוגמה, את הכתובת הפיסית 00-50-04-B4-3A-23 עליך להקליד בתיבה MAC Address את הערך 005004B43A23.
7. בתיבת הטקסט Description הקלד **Reservation made by: <*your name*>**.

   שים לב לכך שניתן להגדיר לקוח DHCP, לקוח BOOTP או את שניהם גם יחד, כך שישתמשו בשמירה זו. לקוח BOOTP יכול להיות התקן כגון מסוף מיושן (Legacy Terminal) או נתב (Router). בקשה של לקוח מסוג זה נענית על ידי שרת DHCP וניתן להוריד נתוני תצורה נוספים. מרחבי BOOTP דינמיים (Dynamic BOOTP Scopes) נתמכים גם הם. למידע נוסף אודות אפשרויות הגדרה אלו, עיין בחלק Supporting BOOTP Clients במערכת העזרה המקוונת של DHCP.
8. בחלק Supported types לחץ על לחצן האפשרויות DHCP Only ולחץ Add. תיבת דו-שיח New Reservation נוספת תיפתח.
9. לחץ Close.
10. שים לב שהשמירה מופיעה בחלונית הפרטים.
11. לחץ על Server01 Scope [192.168.1.0] Scope בחלון Tree.
12. פתח את תפריט Action ולחץ על Activate.

    שים לב שהחץ האדום שמימין לשם המרחב נעלם. שים לב גם לכך שהחץ שליד Server01.microsoft.com [192.168.1.201] עדיין מופיע.

13. לחץ על [192.168.1.201] Server01.microsoft.com בחלון Tree.

14. פתח את תפריט Action ולחץ על Authorize, כדי לאשר את שרת DHCP זה במסד Active Directory (Active Directory Store).

15. הקש על F5, כדי לרענן את התצוגה.

כאשר ליד [192.168.1.201] Server01.microsoft.com מופיע חץ ירוק המורה כלפי מעלה, מציין הדבר כי שירות DHCP אושר.

הליך 6: הגדרת אפשרויות Scope

בהליך זה תגדיר DHCP כך ש-DNS Server המועדף וה-DNS Domain Name יישלחו ללקוח בעת רישומו ברשת. פעולה זו דומה להגדרת אפשרויות השרת, אשר מיושמת בכל לקוחות DHCP המשתמשים בשרת זה, והגדרת אפשרויות ייחודיות ללקוח.

1. בחלון Tree הרחב את [192.168.1.0] Server01.microsoft.com ואת Scope [192.168.1.0], ולחץ על Scope Options.

2. פתח את תפריט Action ולחץ על Configure Options.

 תיבת הדו-שיח Scope Options תופיע.

3. סמן את תיבת הסימון 006 DNS Servers. מתחת Data Entry יופיעו אפשרויות.

4. בתיבת הטקסט Server Name הקלד **Server01**, ולחץ Resolve.

 בתיבה IP Address תופיע הכתובת 192.168.1.201.

5. לחץ Add.

6. גלול את התיבה Available Options, עד שתאתר את הרשומה 015 DNS Domain Name.

7. סמן את תיבת הסימון 015 DNS Domain Name.

8. בתיבה String Value הקלד **microsoft.com** ולחץ OK. נתוני DNS יורדו כעת לכל לקוחות DHCP שב-Scope זה.

9. השאר את תוסף התוכנה של DHCP פתוח; תשתמש בו בהליך הבא.

הליך 7: בדיקת DHCP

בהליך זה תבדוק את שירות DHCP, כדי לוודא שנתוני כתובת IP שהגדרת לצורך שמירה עבור לקוח מופיעים בשרת Server02 וכי חוזה החכירה קיים ב-Server01.

1. ב-Server02, ודא שבתיבת הדו-שיח Internet Protocol (TCP/IP) Properties מסומנים לחצני האפשרויות Obtain an IP address automatically ו- Obtain DNS server address automatically.

   אם אינך בטוח כיצד להשלים צעד זה, חזור לתרגיל 1: "הגדרה ובדיקה של TCP/IP" וסקור שוב את הליך 3 בו.

2. ב-Server02, שחזור את חלון שורת הפקודה (Command Prompt), הקלד בו את הפקודה **ipconfig /renew** והקש Enter. לאחר זמן קצר מוקצית ל-Server02 הכתובת השמורה 192.168.1.76.

3. בשורת הפקודה הקלד **ipconfig /all | more** והקש Enter. שים לב שנתוני DHCP נשלחו למחשב הלקוח. תראה כתובת IP שהוקצתה על ידי שרת DHCP, Subnet Mask, כתובת שרת DNS ושם DNS Domain. נתונים נוספים, כגון Default Gateway, נשלחים בדרך כלל גם הם ללקוח DHCP.

4. כדי לבחון אם Server02 יכול לתקשר עם Server01, הקלד **ping server01**. שים לב ששם השרת משתנה לשם server01.microsoft.com ולכתובת IP שלו. דבר זה אפשרי מכיון שנתוני DNS נשלחו משרת Server01 ל-Server02 כחלק מנתוני DHCP. זוהי תכליתו של שירות DNS.

5. ב-Server01, בחלון Tree של תוסף התוכנה של DHCP, לחץ על Addresses Leases. שים לב שהמחשב server02.microsoft.com מופיע, כאשר כתובת IP שלו היא 192.168.1.76. שים לב גם שליד נתוני חוזה החכירה מופיע Reservation (Active). זאת מכיון שתוקפה של כתובת שמורה אינו פוקע לעולם. לקוח DHCP שאין לו כתובת שמורה, יציג בעמודה Lease Expiration תאריך ושעת פקיעת מועד החוזה.

6. סגור את תוסף התוכנה של DHCP ב-Server01 ואת חלון שורת הפקודה ב-Server02.

גיבוי ושחזור מסד נתוני DHCP

ניתן לערוך את רישום המערכת (System Registry) כדי לקבוע את מרווחי הזמן שבין גיבוי אחד של מסד נתוני DHCP לאחר. בנוסף, ניתן לשחזר מסד נתוני DHCP באופן ידני, על ידי עריכת הרישום.

גיבוי מסד נתוני DHCP

כברירת מחדל, מגבה Windows 2000 את מסד נתוני DHCP בכל 60 דקות. את עותקי הגיבוי היא שומרת בתיקיה %systemroot%\System32\Dhcp\Backup\Jet\new.

ניתן לשנות את פרקי הזמן שבין הגיבויים על ידי שינוי הערך, המייצג את מספר הדקות בין גיבויים, של הרשומה BackupInterval, אותה תמצא במפתח הבא:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters

שחזור מסד נתוני DHCP

כברירת מחדל, שירות DHCP משחזר מסד נתוני DHCP פגום באופן אוטומטי, בעת אתחול השירות. אולם, ניתן לבצע שחזור כזה גם באופן ידני.

כדי לאלץ שחזור מסד נתוני DHCP באופן ידני, ערוך את רישום המערכת (Registry), הגדר את ערך הרשומה RestoreFlag ל-1 ואתחל את השירות. הרשומה RestoreFlag נמצאת במפתח המשנה הבא:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters

---

הערה לאחר ששירות DHCP משחזר בהצלחה את מסד הנתונים שלו, משנה השרת, באופן אוטומטי, את ערך הרשומה RestoreFlag לערך ברירת המחדל - 0.

ניתן גם לשחזר את קובץ מסד נתוני DHCP באופן ידני. כדי לבצע זאת העתק את תוכן התיקיה %systemroot%\System32\Dhcp\Backup\Jet אל התיקיה %systemroot%\System32\Dhcp ואתחל את השירות.

הטבלה הבאה מתארת חלק מהקבצים המאוחסנים בתיקיה %systemroot%\System32\Dhcp :

קובץ	תיאור
Dhcp.mdb	קובץ מסד נתוני DHCP
Tmp.edb	קובץ זמני הנוצר על ידי שירות DHCP עבור נתונים זמניים של מסד הנתונים, כאשר שירות DHCP פעיל.
J50.log and J50*.log	קבצי יומן (Log) הכוללים את כל הפעולות (Transactions) שבוצעו עם מסד הנתונים. מסד נתונים DHCP נעזר בקבצים אלה לצרכי שחזור נתונים, במידת הצורך.

חשוב אל תנסה לשנות את תוכן קבצים אלה, או למחוק אותם!

סיכום שיעור

שירות DHCP של Windows 2000 מרכז ומנהל את מיקום נתוני תצורת TCP/IP, על ידי הקצאת כתובות IP באופן אוטומטי למחשבים המוגדרים כלקוחות DHCP. בכל פעם שלקוח DHCP מאותחל הוא מבקש נתוני מיעון IP משרת DHCP הכוללים כתובת IP, כתובת Subnet Mask וערכים אפשריים נוספים, כגון כתובת Default Gateway. DHCP נעזר בתהליך בן ארבעה שלבים כדי להחכיר נתוני מיעון IP ללקוח DHCP לפרק זמן קצוב מראש : DHCPDISCOVER, DHCPOFFER, DHCPREQUEST ו-DHCPACK. כדי ליישם DHCP עליך, קודם כל, להתקין ולהגדיר את שירות DHCP לפחות במחשב אחד הפועל בסביבת Windows 2000 Server ברשת מבוססת TCP/IP. בנוסף, עליך ליצור ולהפעיל DHCP Scope, שהוא טווח כתובות IP הזמין לחכירה על ידי הלקוחות. עליך גם לאשר את ה-domain בשירותי Active Directory. לאחר שיצרת את מרחב הכתובות, תוכל להגדיר אפשרויות נוספות עבור לקוחות DHCP. קיימות שלוש רמות של אפשרויות : **שרת** (Server), **מרחב** (Scope) ו**לקוח** (Client). עבור חלק מהלקוחות תוכל לבצע שמירה עבור לקוח (Client Reservation), כך ששירות DHCP תמיד יקצה לאותם לקוחות את אותה כתובת IP. תוכל לערוך את רישום המערכת (Registry) כדי להגדיר את פרקי הזמן בהם תגבה Windows 2000 את מסד נתוני DHCP. בנוסף לכך, תוכל גם לשחזר מסד נתוני DHCP באופן ידני, על ידי עריכת רישום המערכת (Registry).

שיעור 4: WINS

שיעור זה מסביר את המטרה והתפקוד של **W**indows **I**nternet **N**aming) WINS **S**ervice) ושל רישום שמות. הוא גם דן בנושא שרת WINS והגדרת לקוח, תמיכה בלקוחות שאינם מפעילים WINS וכיצד להשתמש בתוסף התוכנה (Snap-in) של DHCP להגדרת WINS בלקוח DHCP.

לאחר שיעור זה, תוכל

- להסביר את מטרתה ואופן פעולתה של WINS, כולל רישום שם, חידוש ושחרור שם וגם שאילתת שם.
- ליישם WINS בסביבת Windows 2000.

זמן לימוד משוער: 35 דקות

מבוא ל-WINS

בסביבת רשת מעורבת, לקוחות ברמה-נמוכה (Down-Level Client), כגון מחשבים הפועלים בסביבת Windows 98 או Windows NT 4.0, משתמשים בשמות NetBIOS (Network Basic Input/Output System, לדוגמה "Server01") לצורך ההתקשרות. כתוצאה מכך, רשת Windows 2000 ובה לקוחות ברמה-נמוכה דורשת אמצעים לפתרון שמות NetBIOS לכתובות IP. WINS הוא שרת מורחב לשמות NetBIOS, המבצע רישום של שמות מחשבי NetBIOS ומקשר אותם לכתובות IP. WINS גם מספק מסד נתונים דינמי השומר מיפוי של שמות המחשבים לכתובות IP שלהם.

הערה למידע נוסף אודות WINS פנה לתקליטור המצורף לספר זה, למסמך (\chapt09\articles\wins2000.doc).

הליך קביעת שם של WINS

הליך קביעת השם של WINS מאפשר ללקוחות WINS לרשום את שמם ואת כתובת ה-IP שלהם בשרתי WINS. לקוחות WINS יכולים לבצע שאילתה בשרתי WINS כדי לאתר משאבים אחרים ברשת ולתקשר עמם.

הצעדים הבאים מציגים את תהליך תרגום השמות של WINS :

1. בכל פעם שלקוח WINS מאותחל, הוא רושם את שם NetBIOS ואת מיפוי כתובת ה-IP שלו בשרת WINS ייעודי. אחר כך הוא מבצע בשרת WINS שאילתה לגבי תרגום שם מחשב (Computer Name Resolution).

הערה לקוח WINS **מעדכן באופן אוטומטי את מסד הנתונים בשרת** WINS **בכל פעם שנתוני מיעון** IP **שלו משתנים, למשל, כאשר תוצאת מיעון אוטומטי באמצעות שרת** DHCP **היא כתובת** IP **חדשה למחשב אשר הועבר לרשת משנה שונה.**

2. כאשר לקוח WINS יוזם פקודת NetBIOS כדי לתקשר עם משאב רשת אחר, הוא שולח את הבקשה לשאילתת השם (Name Query Request) ישירות לשרת WINS, במקום לשדר אותה לכל הרשת המקומית.

3. שרת WINS מאתר את שם NetBIOS ומיפוי כתובת IP למשאב היעד במסד הנתונים שלו ומחזיר כתשובה ללקוח WINS את כתובת ה-IP המבוקשת.

הערה שירות WINS **פועל כמו שירות 144 של בזק. לקוחות פונים אליו עם שם המחשב** (NetBIOS) **ומקבלים מספר טלפון** (IP Address).

רישום שם

לכל לקוח WINS מוגדרת כתובת IP של שרת WINS ראשי (Primary WINS Server), וניתן גם להוסיף כתובות שרתי WINS נוספים (סך הכל עד 12 שרתי WINS), אך אין זו חובה. ניתן להגדיר כתובות IP של שרתי WINS בלקוח, באמצעות האפשרויות הנוספות בשרת DHCP. כאשר לקוח מאותחל הוא רושם את שם NetBIOS שלו ואת כתובת ה-IP שהוקצתה לו, על ידי שליחת בקשה לרישום שם (Name Registration Request) ישירות לשרת WINS המוגדר בו.

אם שרת WINS זמין, ואף לקוח אחר לא ביצע כבר רישום של שם זה, משיב שרת WINS ללקוח הודעה על הצלחת הרישום. הודעה זו כוללת את משך הזמן ששם NetBIOS זה יהיה רשום ללקוח. שם זה מופיע בעמודה TTL (**T**ime **T**o **L**ive - אורך חיים). בנוסף, שומר שרת WINS את נתוני שם NetBIOS ומיפוי כתובת ה-IP של הלקוח במסד הנתונים בשרת WINS.

כאשר שם כבר רשום

כאשר מתקבלת בקשה לרישום שם NetBIOS אשר כבר מופיע במסד הנתונים של שרת WINS, שולח שרת WINS בקשה לשאילתת שם לבעלים הרשום הנוכחי של שם זה. שרת WINS שולח את הבקשה שלוש פעמים במרווחי זמן של 500 אלפיות השנייה בין שליחה אחת לאחרת. אם המחשב הרשום הוא מחשב Multihomed (מחשב בו מותקן יותר מכרטיס מתאם רשת אחד, הכרוך לפרוטוקול TCP/IP ויש לו כתובת IP נפרדת עבור כל אחד ממתאמי הרשת), מנסה שרת WINS כל אחת מכתובות ה-IP הרשומות למחשב זה, עד שהוא מקבל תשובה, או עד שניסה את כל כתובות ה-IP.

אם הבעלים הרשום הנוכחי של שם זה משיב בהצלחה לשרת WINS, שולח השרת תשובה שלילית לגבי רישום השם ללקוח WINS המנסה לרשום שם זה פעם נוספת. אולם, אם הבעלים הרשום הנוכחי של השם אינו עונה לשאילתות של שרת WINS, ישלח שרת WINS תגובת הצלחת רישום ללקוח WINS המבקש לרשום את השם.

כאשר שרת WINS אינו זמין

לקוח WIN מנסה שלוש פעמים למצוא שרת WINS ראשי. אם ניסיונותיו נכשלים, לאחר הניסיון השלישי הוא שולח את הבקשה לרישום השם לשרתי WINS המשניים (אם הוגדרו כאלה בלקוח). במידה ולא נמצא שרת WINS זמין, המחשב ישלח Broadcast לכל הרשת.

חידוש שם

שרת WINS רושם את כל שמות NetBIOS על בסיס זמני, כך שמחשבים אחרים יוכלו להשתמש באותם שמות במועד מאוחר יותר, אם בעליו המקוריים של שם מפסיקים את השימוש בו. מאחר שרישום שם לקוח בשרת WINS הוא זמני, לקוח WINS צריך לחדש אותו, או שיפוג תוקף החוזה שלו.

כדי להמשיך ולהשתמש בשם NetBIOS, על מחשב הלקוח לחדש את החוזה לפני שתוקפו פג. אם לקוח אינו מחדש את החוזה, עשוי שרת WINS לאשר את השימוש בשם זה ללקוח WINS אחר.

לקוח WINS עם רישום חדש, מנסה לרענן את החוזה שלו לאחר שעברה שמינית (1/8) ממרווח הזמן המוגדר כזמן ההחכרה (**T**ime **T**o **L**ive - TTL) שלו. אם הלקוח אינו מקבל תגובת רענון שם (Name Refresh), הוא שב ומנסה לרענן את החוזה כל שתי דקות, עד שעוברת מחצית ממרווח TTL שלו.

כאשר עברה מחצית ממרווח TTL, מנסה לקוח WINS לרענן את החוזה באמצעות שרת WINS המשני, אם מוגדר כזה. כאשר הוא עובר לשרת WINS המשני, מנסה הלקוח לרענן את חוזהו כאילו היה זה ניסיונו הראשון - פעם בכל שמינית מרווח TTL עד שיצליח, או עד שתעבור מחצית ממרווח TTL (ארבעה ניסיונות). אז, חוזר לקוח WINS ומנסה את שרת WINS הראשי.

כאשר שרת WINS מקבל בקשה לרענון שם (Name Refresh Request), הוא שולח ללקוח תגובת רענון שם ואיתה מרווח TTL חדש. לאחר שלקוח ריענן את החוזה שלו פעם אחת בהצלחה, הוא ינסה לרענן את החוזה כשעוברת מחצית ממרווח TTL הנוכחי.

שחרור שם

כאשר שמו של לקוח WINS כבר אינו בשימוש, שולח הלקוח לשרת WINS הודעה, בה הוא מורה לו לשחרר את השם. כאשר אתה מכבה את לקוח WINS כראוי, שולח הלקוח לשרת WINS בקשה לשחרור שם עבור כל שם רשום. הבקשה כוללת את כתובת IP של הלקוח ואת שם NetBIOS שלו.

כאשר השרת מקבל את הבקשה לשחרור השם, הוא בוחן את מסד הנתונים שלו ומאתר את השמות המוזכרים בו. אם שרת WINS נתקל בתקלה במסד הנתונים, או אם לשם הרשום ממופה כתובת IP שונה, הוא שולח ללקוח הודעה שלילית בנוגע לשחרור השם. אחרת, ישלח שרת WINS ללקוח תגובה חיובית בנוגע לשחרור השם ואז יסמן את השם במסד הנתונים כפנוי. הודעה זו כוללת את שם NetBIOS המשוחרר ומרווח TTL לו הערך 0 (אפס).

חיפוש שם

לאחר שלקוח WINS רשם את שם NetBIOS שלו ואת כתובת ה-IP שלו בשרת WINS, הוא יכול לתקשר עם מארחים אחרים, על ידי השגת כתובת IP של מחשבים מבוססי-NetBIOS אחרים משרת WINS.

כברירת מחדל מנסה לקוח WINS להסדיר את שמו של מארח NetBIOS אחר ואת כתובת ה-IP שלו באופן הבא:

1. הלקוח בוחן את מטמון שמות NetBIOS שלו ומנסה לאתר את שם NetBIOS/מיפוי כתובת IP של מחשב היעד.
2. אם הלקוח אינו מצליח לפתור את השם מהמטמון שלו, הוא שולח שאילתה לאיתור השם, ישירות לשרת WINS הראשי.
3. אם שרת WINS הראשי אינו זמין, שולח הלקוח בקשה חוזרת פעמיים נוספות לשרת WINS ראשי, ואז הוא עובר לשרתי WINS המשניים.
4. אם אף אחד משרתי WINS המוגדרים בלקוח אינו פותר את השם, הוא שולח בקשה ללקוח בעל כתובת ה-IP, בבקשה לקבל את שם NetBIOS שלו.
5. אם אף שרת WINS אינו מצליח לפתור את השם, מקבל הלקוח הודעה האומרת כי השם המבוקש אינו קיים, ואז הוא מחולל שידור רחב לרשת.
6. אם אין מענה לשידור Broadcast, פונה הלקוח לקובץ LMHOSTS מקומי (במידה והשימוש בקובץ זה הוגדר במאפייני הלקוח).

הערה כל תקשורות WINS מתבצעות באמצעות צרורות נתונים מכוונים (Directed Datagrams) על UDP ב-port 137 (NetBIOS Name Service).

יישום WINS

כדי ליישם WINS, עליך להתקין ולהגדיר אותו בשרת Windows 2000. בנוסף, עליך להגדיר אפשרויות נבחרות במחשבים אשר ישתתפו כלקוחות WINS.

הגדרת שרת WINS

להקמת שרת WINS נדרש מחשב ובו מותקן שרת Windows 2000; אולם, שרת זה אינו חייב להיות Domain Controller. בנוסף, השרת חייב להיות מוגדר עם WINS וצריכים להיות לו כתובת IP קבועה, Subnet Mask ו-Default Gateway .

שרת WINS יכול לכלול גם את התצורות הבאות:

- ❖ מיפוי קבוע לכל הלקוחות שאינם לקוחות WINS (non-WINS Clients), כדי לאפשר תקשורת עם לקוחות WINS ברשתות מרוחקות.
- ❖ תמיכה ב-WINS באמצעות שירות DHCP.

הגדרת לקוח WINS

לקוח WINS חייב לפעול בסביבת אחת ממערכות ההפעלה הבאות:

- ❖ Windows 2000
- ❖ Windows NT Server גירסה 3.51 ומעלה
- ❖ Windows NT Workstation גירסה 3.51 ומעלה
- ❖ Windows 98
- ❖ Windows 95
- ❖ Windows for Workgroups גירסה 3.11 ובה מותקן Microsoft TCP/IP-32
- ❖ MS-DOS ובה מותקן Microsoft Network Client גירסה 3.0 עם מנהל התקן TCP/IP במצב-אמיתי (Real-Mode TCP/IP Driver)
- ❖ LAN Manager גירסה 2.2c עבור MS-DOS (LAN Manager גירסה 2.2c עבור OS/2 אינו נתמך)

ללקוח WINS חייבת להיות מוגדרת כתובת IP של שרת WINS ראשי (Primary WINS Server), ואם קיימים, אז גם של שרתי WINS משניים.

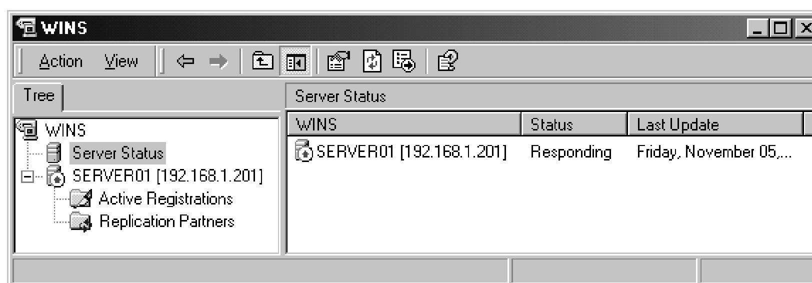
התקנת WINS

שירות WINS (WINS Service) אינו מותקן כחלק מההתקנה הרגילה של שרת Windows 2000. עליך להוסיף את השירות בעצמך, כפי שיתואר להלן. כדי להתקין את שירות WINS השתמש בתוכנית השירות Add/Remove Programs שבלוח הבקרה (Control Panel). לאחר שתתקין את שירות WINS בשרת Windows 2000, תוכל להגדיר את מאפייני TCP/IP שלו כך שהוא יצביע על עצמו. לביצוע הגדרה זו עליך לבחור בכרטיסיה WINS בתיבת הדו-שיח Advanced TCP/IP Settings.

תוסף התוכנה של WINS

תוכל להיעזר בתוסף התוכנה (Snap-in) של WINS, כמו זה המוצג בתרשים 9.8, לכל משימות הניהול וההגדרה של שרת WINS שלך.

תוסף התוכנה של WINS מאפשר גישה לנתונים מפורטים אודות שרתי WINS ברשת. הוא גם מאפשר לך לצפות בתוכן מסד הנתונים של WINS ולחפש אחר רשומות מסוימות.



תרשים 9.8 תוסף התוכנה של WINS.

ניתן לפתוח את תוסף התוכנה של WINS בחלון MMC Console נפרד, או דרך תוסף תוכנת הניהול Computer Management, מתוך Services and Applications. כדי שתוכל להשתמש בתוסף התוכנה של Windows 2000 עליך להתקין קודם את WINS.

תמיכה בלקוח Non-WINS

בסביבת WINS תוכל לספק תמיכה גם ללקוחות שאינם לקוחות WINS, באמצעות מיפוי קבוע או סוכן WINS proxy.

מיפוי קבוע

ברשת הכוללת לקוחות שאינם לקוחות WINS (non-WINS) תוכל להגדיר שם NetBIOS קבוע/מיפוי כתובת IP עבור כל לקוח non-WINS. דבר זה מבטיח שלקוחות WINS יוכלו לתרגם את שמות NetBIOS של לקוחות non-WINS.

הערה אם יש לך לקוחות DHCP הדורשים מיפוי קבוע, עליך לשמור כתובת IP עבור לקוח DHCP, כך שכתובת ה-IP שלו תישאר תמיד קבועה.

כדי להגדיר רשומה קבועה עבור לקוחות non-WINS, פתח את תפריט Action, בחר Active Registration ואז בחר New Static Mapping. כשאתה יוצר מיפוי קבוע, עליך להגדיר מרחב NetBIOS (NetBIOS Scope). מרחב NetBIOS הוא הרחבה אופציונלית לשם מחשב, בה ניתן להשתמש כדי לקבץ מחשבים ברשת.

קיימים חמישה סוגים של מיפוי קבוע (Static Mapping), אותם תוכל ליצור כשאתה מוסיף מיפוי קבוע. חמישה סוגים אלה מתוארים בטבלה הבאה:

אפשרות	תיאור
Unique	שם ייחודי הממופה לכתובת IP יחידה.
Group	שם הממופה לקבוצה. כאשר מוסיפים רשומה לקבוצה באמצעות תוסף התוכנה של WINS, הכנס שם מחשב וכתובת IP. כתובות ה-IP של חברים בקבוצה אינן נשמרות במסד הנתונים של שרת WINS, כך שאין הגבלה למספר החברים שתוכל להוסיף.
Domain Name	מיפוי שם NetBIOS/כתובת IP, כאשר 0x1C הוא הבייט ה-16 שלו. Domain Group מאחסנת עד 25 כתובות עבור החברים בה. רישום של מספר גבוה מזה יגרום ל-WINS לדרוס רישום כתובת משוכפלת, או אם כזו אינה קיימת, לדרוס את הרישום הישן ביותר.
Internet Group	קבוצות המוגדרות על ידי המשתמש (User-defined Groups), בהן תשתמש לקיבוץ משאבים, כגון מדפסות, לצרכי עיון (Browsing). קבוצת אינטרנט יכולה לאחסן עד 25 כתובות של חברים. אולם, חבר דינמי בקבוצה אינו מחליף חבר קבוע שאתה מוסיף באמצעות תוסף התוכנה של WINS או על ידי ייבוא קובץ LMHOSTS.
Multihomed	שם ייחודי אשר יכול לכלול יותר מאשר כתובת IP אחת. השתמש באפשרות זו עבור מחשבים, בהם מותקנים מספר כרטיסי מתאם רשת. ניתן לרשום עד 25 כתובות מרובות בתים (Multihomed Addresses). לרשומות שמעבר לרשומה ה-25, WINS דורסת רישום כתובת משוכפלת, או אם כזו אינה קיימת, יידרס הרישום הישן ביותר.

הערה תוסף התוכנה של WINS מוסיף מיפוי קבוע למסד הנתונים של WINS כאשר אתה לוחץ OK. אם הוספת נתוני מיפוי קבוע שגויים, עליך למחוק מיפוי זה ואז ליצור אחד חדש.

הגדרת WINS Proxy Agent

WINS Proxy Agent מרחיב את אפשרויות פתרון השמות של שרת WINS לצורך טיפול בלקוחות non-WINS, על ידי האזנה לרישומי שמות משודרים (Broadcast Name Registrations) ושידורי בקשות לפתרון שמות (Broadcast Resolution Requests), ואז העברתם לשרת WINS.

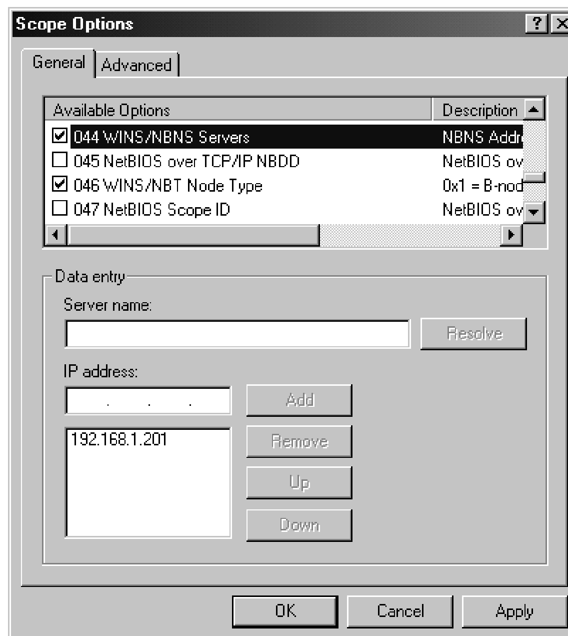
- **רישום שם NetBIOS** (NetBIOS Name Registration) – כאשר לקוח non-WINS משדר בקשה לרישום שם, WINS Proxy Agent מעביר את הבקשה לשרת WINS, כדי לוודא שאף לקוח WINS אחר לא רשם כבר את השם המבוקש. שם NetBIOS אינו נרשם - הוא רק נבדק.
- **פתרון שם NetBIOS** (NetBIOS Name Resolution) – כאשר WINS Proxy Agent מזהה שידור רחב לפתרון שם (Name Resolution Broadcast), הוא בוחן את מטמון שמות NetBIOS שלו ומנסה להסדיר את השם. אם השם המבוקש אינו מופיע במטמון, נשלחת הבקשה לשרת WINS. שרת WINS שולח ל-WINS Proxy Agent שלו כתובת IP עבור שם NetBIOS המבוקש. הסוכן הוא זה המשיב את הכתובת לאותו לקוח non-WINS.

כדי להגדיר WINS Proxy Agent, ערוך את רישום המערכת (Registry) בלקוח המאפשר WINS - הגדר בו את ערך הרשומה EnableProxy ל-1 ואז אתחל את המחשב. את הרשומה EnableProxy תמצא ברישום המערכת (Registry) תחת מפתח המשנה –

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters

הגדרת אפשרויות WINS בשרת DHCP

אם מחשב הוא לקוח DHCP תוכל להגדיר בו תמיכת WINS, על ידי תוסף התוכנה של DHCP. תוסף התוכנה מאפשר לך להוסיף ולהגדיר את האפשרות 044 WINS/NBNS Servers ב-DHCP Scope, ולהגדיר את כתובת WINS לשרת ראשי ולשרתים המשניים (ראה תרשים 9.9).



תרשים 9.9 תיבת הדו-שיח Scope Options בתוסף התוכנה של DHCP.

כאשר לקוח DHCP חוכר או מחדש חוזה חכירה לכתובת, הוא מקבל את אפשרות ה-Scope הזה, והלקוח מוגדר לתמיכה ב-WINS.

הערה אם אתה מגדיר מחשב לקוח עם כתובות IP לשרת WINS, יקבלו ערכים אלה קדימות לעומת אותם ערכים המתקבלים על ידי שרת DHCP.

אתה יכול גם להגדיר את האפשרות 046 WINS/NBT Node Type כדי לקבוע את סוג הצומת. סוגי צמתים אפשריים הם : B-node, P-node, M-node ו- H-node.

הערה למידע נוסף אודות סוגי צמתים קרא את RFC 1001 ו-RFC 1002. **RFC** (Request for Comment) הוא מסמך בו מפורסם מידע אודות תקן, פרוטוקול או מידע אחר הקשור לפעילותה של רשת האינטרנט. מסמך RFC מפורסם לאחר דיונים ומשמש כתקן למעשה. תוכל למצוא את נוסחו של כל RFC המוזכר בספר זה (כמו גם מסמכי RFC רבים נוספים הקשורים לנושאים הנידונים בספר) באינטרנט. היעזר בדפדפן האינטרנט שלך כדי לבצע חיפוש אחר RFC המעניינים אותך. במקרה זה חפש אחר "RFC 1001" או "RFC 1002". דוגמה לאתר היא http://www.nexor.com/info/rfc/index/rfc.htm?index/rfc.htm, או לחילופין נסה את הכתובת http://www.sri.ucl.ac.be/normes/rfc.html. אלה הם מנועי חיפוש למסמכי RFC.

תרגיל 3: התקנה והגדרת WINS

בתרגיל זה תתקין WINS בשרת Server01. לאחר ההתקנה יוגדרו הגדרות נוספות כדי ששירות DHCP יתמוך ב-WINS. ודא כי תקליטור ההתקנה המקורי של Windows 2000 Server נמצא ב- Server01.

הערה WINS נדרש רק לצרכי תאימות לאחור (Legacy Support). ברשת התרגול המצומצמת שלך, וברשת הומוגנית בה כל הלקוחות והשרתים פועלים בסביבת Windows 2000, אין צורך ב-WINS, מפני שכל מחשב הפועל בסביבת Windows 2000 משתמש ב-DNS לצורך פתרון השמות. תרגיל זה נועד לתרגול ביצוע משימות בסיסיות, כגון התקנה והגדרה של WINS.

הליך 1: התקנת WINS

בהליך זה תתקין את WINS ב-Server01.

1. היכנס ל-Server01 בשם משתמש Administrator ועם הסיסמה password.
2. לחץ Start, הצבע על Settings ולחץ על Control Panel.
3. לחץ לחיצה כפולה על הסמל Add/Remove Programs.

   חלון Add/Remove Programs יופיע.
4. לחץ על Add/Remove Windows Components בחלונית השמאלית.
5. בתיבה Components, לחץ על Networking Services, אבל אל תשנה את מצב תיבת הסימון שמשמאל לאפשרות זו.
6. לחץ Details. תיבת הדו-שיח Networking Services תופיע.

   בתיבה Subcomponents of networking services סמן את תיבת הסימון שליד האפשרות Windows Internet Naming Service (WINS).
7. לחץ OK. יופיע מסך Windows Components.
8. לחץ Next. המסך Configuring Components מבצע את שינויי ההגדרות שביקשת. תיבת File Copy תופיע כאשר קבצי WINS מועתקים לתיקיות מערכת ההפעלה במחשב. כעת יופיע המסך Completing the Windows Components Wizard.
9. לחץ Finish.
10. סגור את חלון Add/Remove Programs.
11. סגור את חלון Control Panel.

הליך 2: הגדרת DHCP לתמיכה ב-WINS

בהליך זה תגדיר את WINS בתוסף התוכנה של DHCP ב-Server01. כדי שתוכל לתרגל את אפשרויות השרת תשתמש בצומת Server Options. הגדרות אלו ניתן לבצע גם כאפשרויות מרחב (Scope Options), אם אתה מעוניין שהן יוחלו רק על מרחב מסוים או אפילו רק ללקוח DHCP מסוים.

1. פתח את תוסף התוכנה של DHCP בשרת Server01.
2. בחלון Tree לחץ על Server Options.
3. קרא את ההודעה המופיעה בחלונית הפרטים.
4. פתח את תפריט Action ובחר באפשרות Configure Options.

   תיבת הדו-שיח Server Options תופיע.
5. גלול כלפי מטה עד שתראה את האפשרות 044 WINS/NBNS Servers מופיעה. סמן את תיבת הסימון הזו.
6. בתיבת הטקסט Server Name הקלד **Server01** ולחץ Resolve.

   בתיבה IP Address תופיע כתובת ה-IP של Server01, 192.168.1.201.
7. לחץ Add.
8. בתיבה Available Options גלול כלפי מטה עד שתראה את תיבת הסימון 046 WINS/NBT Node Type. סמן את התיבה.
9. בתיבת הטקסט Byte הקלד את הערך **8**, כך שהערך שיופיע בה יהיה 0x8.

   0x8 מגדיר את סוג הצומת ל- H-node. סוג הצומת קובע כיצד תתבצע הסדרת WINS במחשב הלקוח. H-node מורה ללקוח קודם כל לבדוק בשרת WINS (P-node התקשרויות נקודה-לנקודה עם שרת שמות) ואחר כך לשלוח שידור B-node, במידת הצורך.
10. לחץ על OK. שתי אפשרויות השרת מופיעות בחלונית הפרטים.
11. סגור את תוסף התוכנה של DHCP.

הליך 3: בדיקת הגדרות WINS (לא חובה)

בהליך זה תשחרר ותחדש את חוזה חכירת DHCP ב-Server02. אז תטען את תוסף התוכנה של WINS ב-Server01, כדי לבחון את הרישום של Server02 במסד הנתונים של WINS.

הערה אם רק אתחלת את Server02 דלג ישירות לצעד 4. שלושת הצעדים הראשונים דרושים רק כדי לעדכן את חכירת DHCP.

---

1. ב-Server02 פתח חלון שורת הפקודה (Command Prompt).
2. הקלד **ipconfig /release** והקש Enter. ,תופיע הודעה המורה כי כתובת ה-IP שוחררה בהצלחה מהמתאם Local Area Connection.
3. הקלד **ipconfig /renew** והקש Enter. הגדרות IP מופיעות כאשר החוזה מחודש.
4. הקלד **ipconfig /all | more** והקש Enter.
5. הקש Enter כמה פעמים שנדרש, כדי לבחון את ההגדרות עבור <adapter type> adapter Local Area Connection.
6. שים לב שסוג הצומת מוגדר Hybrid. Hybrid הוא המקביל לצומת H-node. בנוסף, שים לב ששרת WINS הראשי מוגדר לכתובת 192.168.1.201, שהיא כתובת ה-IP של Server01.
7. סגור את חלון שורת הפקודה ב-Server02.
8. ב-Server01 לחץ Start, הצבע על Programs, הצבע על Administrative Tools ולחץ על WINS. מופיע תוסף התוכנה של WINS.
9. הגדל את תוסף התוכנה WINS לגודלו המירבי.
10. הרחב את [192.168.1.201] SERVER01 ולחץ על Active Registrations.
11. קרא את ההודעה המופיעה בחלונית הפרטים.
12. פתח את תפריט Action ובחר Find By Name. תיבת הדו-שיח Find By Name תופיע.
13. בתיבת הטקסט Find Names Beginning With (אתר שמות המתחילים ב...) הקלד **Ser**, ולחץ Find Now.

    בעמודה Record Name יופיע Server02 עם שלוש רשומות. שלוש רשומות אלו הן השירותים המשדרים את שמו של Server02 לרשת. הרשומה הראשונה, 00h, היא שם NetBIOS של המחשב. 03h משמשת לשליחה ולקבלת הודעות משודרות. 20h משמש לצורך שיתוף גישה עם מחשבים אחרים ברשת.
14. סגור את תוסף התוכנה של WINS.

סיכום שיעור

רישום שמות הוא חלק חשוב בתהליך הסדרת השמות (Name Resolution). לכל לקוח WINS מוגדרת כתובת שרת WINS ראשי, ואם קיימים אז גם כתובות שרתי WINS משניים. בכל פעם שלקוח WINS מאותחל, הוא רושם את שם NetBIOS שלו ואת כתובת ה-IP, על ידי שליחת בקשה לרישום ישירות לשרת WINS המוגדר בו. שרת WINS רושם את כל שמות NetBIOS על בסיס זמני, כך שלקוח WINS חייב לחדש את שמו, או שתוקף החוזה שלו יפוג. כאשר שרת WINS מקבל את הבקשה לרענון השם, הוא משיב ללקוח בהודעת רענון הכוללת גם את מרווח ה-TTL (Time To Live) החדש שלו. בנוסף, כאשר שם לקוח WINS כבר אינו בשימוש שולח הלקוח הודעת שחרור לשרת. כששרת WINS מקבל בקשה לשחרור השם, הוא בוחן את מסד הנתונים שלו ומאתר את שם NetBIOS המדובר. אם הוא מאתר את NetBIOS name/IP address המתאימים במסד הנתונים שלו, הוא שולח תגובה חיובית לשחרור, ומסמן את השם במסד הנתונים כמשוחרר. כדי ליישם WINS עליך להתקין ולהגדיר את WINS בשרת Windows 2000. בנוסף להתקנת WINS, עליך להגדיר מספר אפשרויות נבחרות במחשבים שאמורים להיות לקוחות WINS. תוסף התוכנה של WINS מאפשר גישה לנתונים מפורטים אודות שרתי WINS ברשת, ומאפשר לך לצפות בתוכן מסד הנתונים של WINS ולחפש בו אחר רשומות ספציפיות.

שיעור 5: DNS

DNS (**D**omain **N**ame **S**ystem) הוא מסד נתונים מבוזר (Distributed Database), המשמש ברשתות TCP/IP כדי לתרגם שמות מחשבים (שמות מארחים, Host Names) לכתובות IP. שיעור זה מציג בפניך את DNS ונושא הסדרת השמות (Name Resolution). הוא גם דן במיומנויות הנדרשות ומספק מידע אודות אופן ההתקנה והגדרה של שירותי DNS.

לאחר שיעור זה, תוכל

- **להסביר את אופן פעולתו של** DNS **ומרכיביו, ולהסביר את תהליך פתרון השמות.**
- **להתקין ולהגדיר את שירות** DNS, **כולל** Dynamic DNS **ושירות** DHCP **עבור** DNS.
- **להגדיר לקוח** DNS.
- **לאתר תקלות בשירות** DNS.

זמן לימוד משוער: 90 דקות

מבוא ל- DNS

DNS Domain משויך בדרך כלל לאינטרנט. אולם, רשתות פרטיות עושות שימוש נרחב ב-DNS כדי לפתור את שמות המחשבים ולאתר מחשבים ברשת המקומית שלהם, וגם באינטרנט. פתרון שמות באמצעות DNS, שונה מזו המתאפשרת בעת השימוש ב-WINS. WINS פותר שמות NetBIOS לכתובות IP, בעוד ש-DNS פותר, או ממיר, שמות מחשבים מארחי IP (IP Host Computers) לכתובות IP.

למחשבים מארחי שמות IP (IP Host Names) ששמם תורגם באמצעות DNS, או באמצעים אחרים, יש יתרונות כדלקמן:

- שמותיהם של מחשבים מארחי IP (IP Hosts) ידידותיים למשתמש ולכן הם קלים יותר לזכירה מאשר כתובות IP.
- שמותיהם של מחשבים מארחי IP קבועים יותר מאשר כתובות IP. IP Address של שרת יכולה להשתנות כאשר מעבירים אותו לרשת אחרת, אך שמו נשאר ללא שינוי.
- שמותיהם של מחשבים מארחי IP מאפשרים למשתמשים להתחבר לשרתים מקומיים באמצעות מוסכמת השמות הנהוגה באינטרנט.

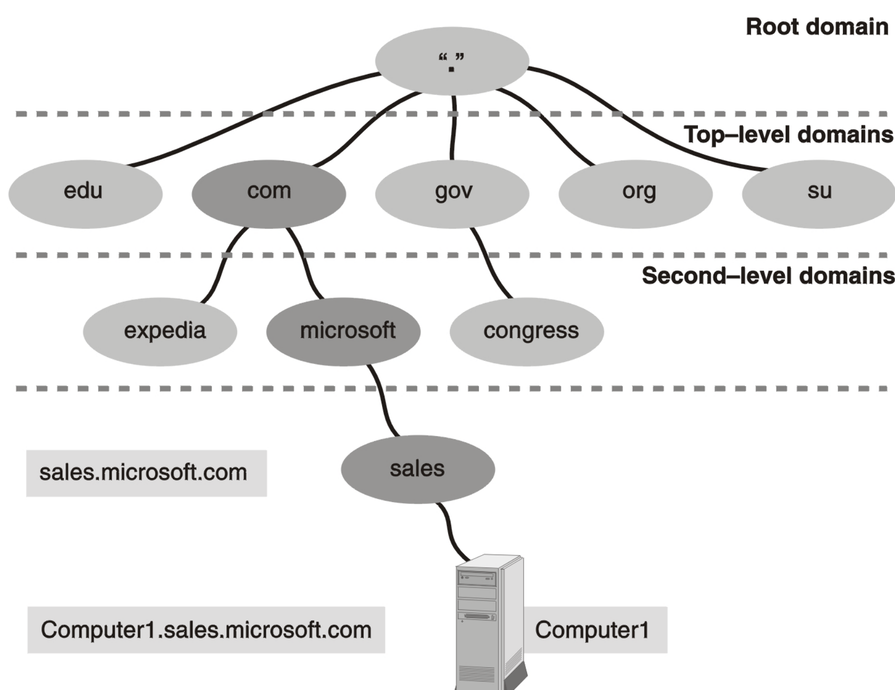
הערה DNS מקשר בין שם "אינטרנטי" לכתובת IP **ובכך מקל עלינו. במקום לזכור את** כתובת ה-IP של הוצאת הוד-עמי, שהיא 208.56.239.22 **יש לזכור** www.hod-ami.co.il **וזה** הרבה יותר קל.

הערה למידע נוסף אודות DNS קרא את RFC 1034 **ואת** RFC 1035. היעזר בדפדפן האינטרנט שלך כדי לחפש אחר הערכים "RFC 1034" **ו-**"RFC 1035". מידע נוסף אודות DNS **ויישומו** תוכל למצוא בתקליטור המצורף לספר זה: (\chapt09\articles\w2kDNS.doc).

Domain Namespace

Domain Namespace - שיטה של מתן שמות המספקת את המבנה ההיררכי למסד נתוני DNS. כל צומת (Node) מייצג מחיצה של מסד נתוני DNS. לצמתים אלה מתייחסים כאל Domain.

מסד נתוני DNS ממויין על פי שם; בשל כך, לכל Domain חייב להיות שם. כשתתאם מוסיף Domains למבנה ההיררכי מצורף שם Parent Domain לשם Child Domain, הנקרא גם Subdomain. כתוצאה מכך, שמו של ה-Domain מזהה את מיקומו במבנה ההיררכי. לדוגמה, בתרשים 9.10 ה-domain ששמו sales.microsoft.com מזהה את ה-Domain ששמו sales כ-subdomain של ה-Domain בשם microsoft, ואת ה-Domain microsoft כ-Subdomain של ה-Domain ששמו com.



תרשים 9.10 מבנה היררכי של Domain Namespace.

כפי שמתואר בתרשים 9.10, המבנה ההיררכי של ה-Domain Namespace כולל Root Domain, Top-level domains, Second-level domains ו-Host names.

הערה למונח Domain, בהקשרו לנושא DNS, **יש מובן מעט שונה מזה הקשור לנושא** Directory Services **של** Windows 2000. Windows 2000 Domain **הוא קיבוץ מספר מחשבים והתקנים המנוהלים כיחידה אחת. בהקשרו ל-**DNS, ה-Domain **הוא צומת המייצג מחיצה במסד הנתונים של** DNS.

Root Domain

Root Domain נמצא ברומו של המבנה ההיררכי ומיוצג על ידי נקודה (.). ה-Root Domain של האינטרנט מנוהל על ידי מספר ארגונים, כגון Network Solutions, Inc.

Top-Level Domains

Top-level domains הם קוד בן שניים או שלושה תווים ומחולקים ומאורגנים על פי שמות הארגונים או מיקומם הגיאוגרפי. הטבלה הבאה מציגה דוגמאות ל-Top-level domains:

Top-level domains	תיאור
gov	ארגונים ממשלתיים
com	ארגונים מסחריים
edu	מוסדות חינוך
org	מוסדות ללא כוונת רווח
au	קוד מדינה עבור אוסטרליה

Top-level domains יכולים לכלול Second-level domains ו-Host names.

Second-Level Domains

ארגונים כגון Network Solutions Inc. רושמים Second-level domains עבור ארגונים, חברות ואנשים פרטיים לשימוש באינטרנט. Second-level domain יכול לכלול Hosts וגם Subdomains. לדוגמה, microsoft.com יכול לכלול מחשבים כגון ftp.microsoft.com ו-Subdomains כגון dev.microsoft.com. Subdomain בשם dev.microsoft.com יכול לכלול Hosts כגון printerserver1.dev.microsoft.com.

Host Names

Host Names מתייחסים לשמות ספציפיים של מחשבים באינטרנט או ברשת הארגונית. לדוגמה, בתרשים 9.10 Computer1 הוא שם host. Host name הוא החלק השמאלי ביותר של **F**ully **Q**ualified **D**omain **N**ame - FQDN, אשר מתאר את מיקומו המדויק של ה-host במבנה ההיררכי של ה-domain. בתרשים 9.10, Computer1.sales.microsoft.com. (כולל הנקודה, אשר מייצגת את ה-Root Domain) הוא FQDN.

DNS משתמש ב-FQDN של המארח כדי להמיר את השם לכתובת IP.

הערה Host name אינו חייב להיות זהה לשם המחשב. כברירת מחדל, התקנת TCP/IP משתמשת בשם המחשב כשם ה-host שלו, כשהיא מחליפה תווים שאינם חוקיים, כגון קו תחתון (_), במקפים (-). קרא את RFC 1035.

הנחיות למתן Domain Name

כשאתה יוצר Domain Namespace, עליך להתחשב בקווים המנחים ובמוסכמות מתן השמות הבאות:

- הגבל את מספר הרמות ב-Domain. בדרך כלל רשומות מארחי DNS צריכות להיות שלוש או ארבע רמות ברמת ההירכיה של DNS, ולא יותר מאשר חמש רמות מתחת לרמת השורש. ככל שמספר הרמות גדל, כך גדלות גם משימות הניהול.
- השתמש בשמות ייחודיים. לכל Subdomain צריך להיות שם ייחודי ב-Parent Domain שלו, כדי להבטיח שהשם הוא ייחודי בכל ה-DNS Namespace.
- השתמש בשמות פשוטים. שמות Domain פשוטים וברורים קלים יותר לזכירה של המשתמשים, מאפשרים להם לבצע חיפוש אינטואיטיבי, לאתר אתרי אינטרנט או מחשבים אחרים באינטרנט או באינטראנט.
- הימנע משמות domain ארוכים. Domain Names יכולים להכיל עד 63 תווים, כולל הנקודות. אורכו של FQDN אינו יכול להיות מעבר ל-255 תווים. שמות Domain אינם רגישים לגודל אותיות רישיות (non Case-sensitive).
- השתמש רק בתווי DNS ותווי Unicode תקניים:

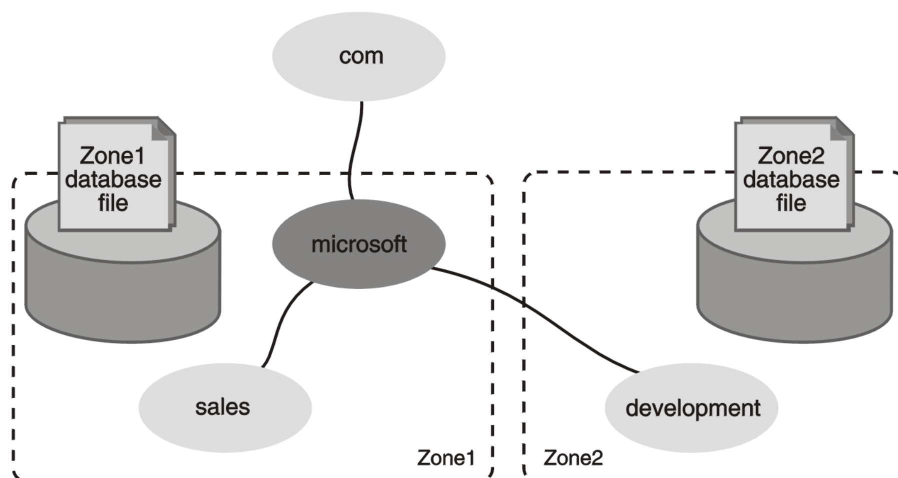
  - Windows 2000 תומכת בתווי DNS התקניים הבאים: A עד Z, a עד z, 0 עד 9, ומקף (-), כפי שמוגדר בקובץ RFC 1035.
  - שירות DNS גם תומך בקובץ תווי Unicode. קובץ תווי Unicode, הכולל מספר תווים שאינם מופיעים כחלק מתקן ASCII (**A**merican **S**tandard **C**ode for **I**nformation Exchange), נדרש עבור שפות כגון צרפתית, גרמנית וספרדית.

הערה השתמש בתווי Unicode רק אם כל השרתים בסביבתך, בהם פועל שירות DNS תומכים בתקן Unicode. למידע נוסף אודות תקן Unicode וקובץ התווים שלו, קרא את RFC 2044, על ידי חיפוש אחר הערך "RFC 2044" באמצעות דפדפן האינטרנט שלך.

Zones

אזור (Zone) מתייחס לחלק נפרד אך המשכי בטווח השם. יצירת אזורים (Zones) מאפשרת חלוקה למחיצות של ה-Domain Namespace למקטעים קלים לניהול.

ריבוי אזורים ב-Domain Namespace משמש להפצת משימות ניהול לקבוצות שונות. לדוגמה, תרשים 9.11 מתאר את ה-Domain Namespace של Domain ושמו microsoft.com כאשר הוא מחולק לשני אזורים. שני האזורים מאפשרים למנהל (Administrator) אחד לנהל את ה-Domains : microsoft ו-sales, ולמנהל (Administrator) אחר לנהל את ה-Domain ושמו development.



תרשים 9.11 Domain namespace מחולק לשני אזורים.

Zone חייב להקיף Domain Namespace רציף. לדוגמה, כפי שניתן לראות בתרשים 9.11, ביכולתך ליצור Zone עבור sales.microsoft.com ועבור ה-Parent Domain ושמו microsoft.com מפני ששני ה-Domains רציפים. אולם, אינך יכול ליצור אזור הכולל רק את ה-Domains : sales.microsoft.com ו- development.microsoft.com, מבלי להתייחס ל-Parent Domain.

מיפויי שם-לכתובת IP עבור אזורים נשמרים בקובץ מסד נתוני האזור. כל אזור מעוגן ל-Domain מסוים, אשר הייחוס אליו הוא כאל Zone's Root Domain. קובץ מסד נתוני האזור אינו מכיל בהכרח נתונים עבור כל ה-Subdomains של ה-Zones root domain, אלא רק את אלו של ה-Subdomains שהם חלק מהאזור.

בתרשים 9.11, ה-Root domain עבור Zone1 הוא microsoft, וקובץ האזור מכיל את מיפוי השם-לכתובת-IP עבור ה-Domains : microsoft ו-sales. קובץ האזור עבור Zone1 אינו מכיל את מיפוי השם-לכתובת-IP עבור ה-Domain ששמו development, למרות ש-development הוא Subdomain של ה-Domain - microsoft.

DNS Name Servers

שרת שמות DNS מאחסן את קובץ מסד נתוני האזור. שרתי שמות (Name Servers) יכולים לאחסן נתונים של אזור אחד, או של מספר אזורים. לשרת שמות אמורה להיות הרשאה ל-Domain Namespace הכלול באזור (Zone).

חייב להיות לפחות שרת שמות אחד באזור. אולם, לאזור יכולים להיות מספר שרתי שמות משניים המשויכים אליו. אחד מהשרתים מכיל את הקובץ הראשי של מסד נתוני האזור (Master Zone Database File, הנקרא גם Primary Zone Database File) עבור אותו אזור. שינויים לאזור, כגון הוספת Domains או מחשבי מארח (Hosts), מבוצעים כולם בשרת המכיל את הקובץ הראשי של מסד נתוני האזור. שרתי שמות משניים המשויכים לאזור, משמשים כגיבוי לשרת השמות, המכיל את הקובץ הראשי של מסד נתוני האזור. שרתים אלה מכילים קובץ גיבוי (Read Only) לקובץ מסד נתוני האזור הראשי.

Windows 2000 תומכת גם באחסון אזורים משולב בספריית הרשת. שרת DNS הפועל על בקר Domain (Domain Controller), ניתן להגדיר את ה-Zone שלו כ-Active Directory Integrated. אזור משולב שומר את המידע בספריה האקטיבית ולא כקובץ טקסט בשרת. לפיכך גם שכפול נתוני האזור נעשה כחלק משכפול נתוני Active Directory ואין צורך בהעברת נתונים נוספת.

להגדרת מספר שרתי שמות היתרונות הבאים:

- **ביצוע מעברי אזורים** (Zone Transfers) – שרתי השמות המשניים משיגים עותק של קובץ מסד נתוני האזור משרת השמות הראשי, המכיל את הקובץ הראשי של מסד Zone Transfer. דבר זה נקרא מעבר אזורים. שרתי שמות אלה מבצעים מדי פעם שאילתה בשרת השמות הראשי, כדי לקבל עדכונים של קובץ מסד נתוני האזור.
- **מספקים יתירות** (Redundancy) – אם שרת השמות המכיל את הקובץ הראשי של מסד נתוני האזור "נופל", יכולים השרתים המשניים לספק את השירות.
- **משפרים את מהירות הגישה עבור מיקומים מרוחקים** – אם מספר לקוחות נמצאים במיקום מרוחק, השתמש במספר שרתי שמות משניים כדי להקטין את תעבורת השאילתות (Query Traffic) דרך קישורי WAN איטיים.
- **הפחתת עומסים** – שרתי השמות המשניים מפחיתים את העומס על שרת השמות, המכיל את הקובץ הראשי של מסד נתוני האזור בכך שהשאילתות אינן מתנקזות לשרת אחד בלבד.

Name Resolution

הסדרת שמות (Name Resolution) הוא התהליך בו מומרים שמות לכתובות IP. הסדרת השמות דומה לחיפוש שם במדריך הטלפונים, כאשר השם משויך למספר טלפון. לדוגמה, כאשר אתה מתחבר לאתר האינטרנט של Microsoft אתה משתמש בשם www.microsoft.com. DNS ממיר את השם www.microsoft.com לכתובת ה-IP המשויכת לו. מיפוי השמות לכתובות ה-IP מאוחסן במסד הנתונים המבוזר של DNS.

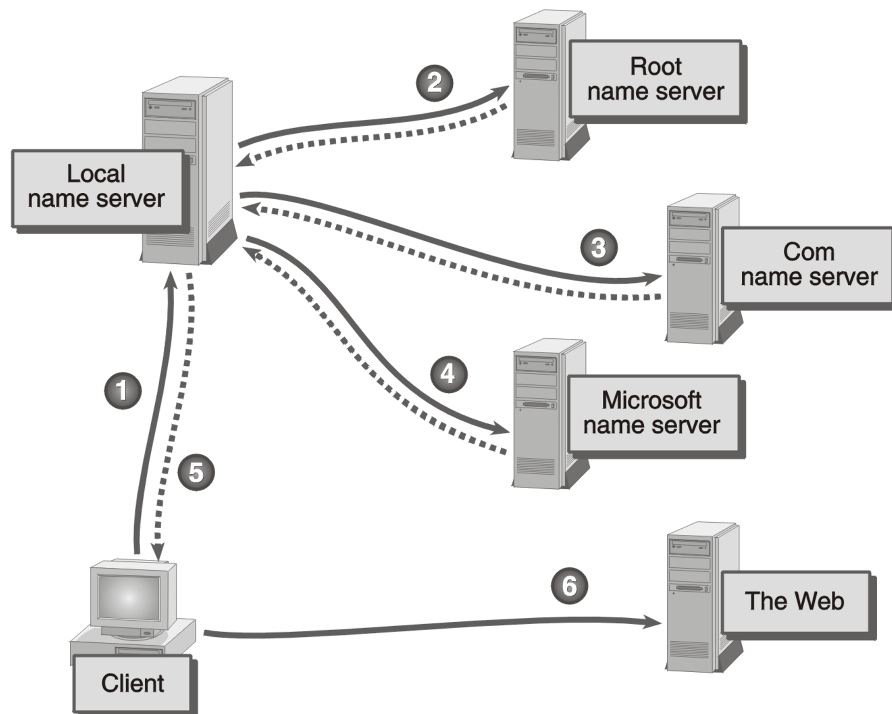
שרתי שמות של DNS מסדירים שאילתות חיפוש דו-כיווניות. שאילתה המחפשת לפנים (Forward Lookup Query) ממירה שם לכתובת IP. שאילתה המחפשת לאחור (Reverse Lookup Query) ממירה כתובת IP לשם. שרת שמות יכול להמיר שאילתה רק עבור אזור בו יש לו סמכות (Authority). אם שרת שמות אינו מסוגל להמיר שאילתה הוא מעביר אותה הלאה, לשרתי שמות אשר מסוגלים לבצע זאת. שרת השמות שומר בזיכרון מטמון (Cache) את תוצאות השאילתה כדי להפחית את תעבורת DNS ברשת.

Forward Lookup Query

שירות DNS משתמש במודל שרת/לקוח עבור Name Resolution (פתרון שמות). כדי לפתור שאילתה המחפשת לפנים (Forward Lookup Query) מעביר הלקוח שאילתה לשרת שמות מקומי (Local name server). שרת השמות המקומי פותר (ממיר) את

השאילתה בעצמו, או שהוא שולח שאילתה לשרת שמות אחר כדי להשלים את התהליך.

תרשים 9.12 מתאר את התהליך בו לקוח מבצע שאילתה בשרת השמות עבור כתובת ה-IP של www.microsoft.com. המספרים בתרשים מתוארים בצעדים המופיעים לאחר התרשים.



תרשים 9.12 הסדרת שאילתה המחפשת לפנים.

1. הלקוח מעביר לשרת השמות המקומי שלו שאילתה המבקשת לפתור כתובת IP משרת מארח www.microsoft.com.
2. שרת השמות המקומי בוחן את קובץ מסד נתוני האזור שלו, כדי לקבוע אם הוא מכיל את מיפוי שם-לכתובת-IP לפי שאילתת הלקוח. מכיון שלשרת השמות המקומי אין סמכות ב-Domain עבור השם microsoft.com, הוא מעביר את השאילתה לשרת שורש בהירררכיית DNS, ומבקש ממנו פתרון כתובת IP לשם המארח. שרת שמות השורש שולח חזרה הפניה מיוחסת לכתובתו של שרת השמות com.
3. שרת השמות המקומי שולח בקשה לשרת השמות של com, אשר מגיב בהפניה מיוחסת לשרתי השמות המוסמכים לפתור שמות DNS של Microsoft.

4. שרת השמות המקומי שולח בקשה לשרת השמות של Microsoft. שרת השמות של Microsoft מקבל את הבקשה. מכיון שלשרת השמות של Microsoft יש הרשאה עבור חלק זה של ה-Domain namespace, הוא משיב לשרת השמות המקומי את כתובת ה-IP עבור www.microsoft.com.
5. שרת השמות המקומי שולח את כתובת ה-IP של www.microsoft.com ללקוח.
6. פתרון השם הושלם, וכעת יכול הלקוח לגשת אל www.microsoft.com באמצעות כתובת ה-IP.

Name Server Caching

כאשר שרת שמות (Name Server) מעבד שאילתה עשוי להימצא צורך לשלוח מספר שאילתות אחרות כדי למצוא את התשובה. בכל שאילתה מחפש שרת השמות שרתי שמות נוספים, להם יש הרשאות לחלק מה-Domain namespace. שרת השמות שומר (Caches) תוצאות אלו כדי להפחית את תעבורת הרשת.

כששרת השמות מקבל תוצאה לשאילתה, יבוצעו הפעולות הבאות:

1. שרת השמות שומר (Cache) את תוצאת השאילתה למשך זמן מסוים, המכונה אורך חיים (TTL). האזור שסיפק את תוצאת השאילתה הוא זה אשר קובע את משך ה-TTL. TTL מוגדר באמצעות תוסף התוכנה של DNS. ערך ברירת המחדל שלו הוא 60 דקות.
2. לאחר ששרת השמות שומר את תוצאת השאילתה, מתחילה הספירה לאחור של טווח ה-TTL המקורי.
3. כאשר מסתיים טווח TTL, מוחק שרת השמות את תוצאת השאילתה מהמטמון (Cache) שלו.

שמירת תוצאות שאילתה ב-Cache, מאפשרת לשרת השמות לפתור במהירות שאילתות אחרות, המתייחסות לאותו חלק של ה-Domain namespace.

הערה הגדר ערכים קצרים יותר עבור TTL, כדי להבטיח שהנתונים אודות ה-Domain Namespace יהיו כמה שיותר עדכניים. למרות שערכי TTL קצרים מגבירים את העומס על שרתי השמות, וערכי TTL ארוכים יותר מקצרים את משך הזמן הדרוש למתן מענה לשאילתות ולפתרון שמות, הלקוח לא יקבל את הנתונים המעודכנים עד שיפוג תוקף ה-TTL ותבוצע שאילתה חדשה לאותו חלק של ה-Domain Namespace.

Reverse Lookup Query

שאילתה המחפשת לאחור (Reverse Lookup Query) ממפה כתובת IP לשם מארח. כלים לאבחון תקלות, כגון תוכנית שורת הפקודה nslookup, נעזרת בשאילתה מסוג זה כדי לדווח שמות מארחים (Host names). בנוסף, יישומים מסוימים מיישמים אבטחת מידע, המבוססת על היכולת להתחבר לשמות ולא לכתובות IP.

מאחר שמסד הנתונים המבוזר של DNS ממוין לפי שם ולא לפי כתובת IP, שאילתה המחפשת לאחור תדרוש חיפוש מייגע בכל שמות ה-Domains. כדי לפתור בעיה זו נוצר Domain אשר שמו in-addr.arpa.

ה-Domain ששמו in-addr.arpa עוקב אחר אותה שיטה היררכית למתן שמות כמו שאר ה-Domain namespace; אולם, הוא מבוסס על כתובות IP ולא על שמות Domains, כפי שמתואר בקווים כלליים להלן:

- ❖ Subdomains נקראים אחרי המספרים בתצוגת המספרים המופרדים בנקודות עשרוניות, שבמבנה כתובת IP.
- ❖ סדר האוקטטים של כתובת IP הפוך.
- ❖ חברות מנהלות את ה-Subdomains שלהן ב-Domain ששמו in-addr.arpa בהתבסס על כתובות IP שהוקצו להן ו-Subnet Mask.

לדוגמה, לחברה לה הוקצה טווח הכתובות 192.254.16.0 עד 192.254.16.255, עם Subnet Mask בערכים 255.255.255.0 יש הרשאה לפעול ב-Domain בשם 16.254.192.in-addr.arpa.

התקנת שירות DNS

כדי ליישם DNS עליך להגדיר את השרת ולהתקין את שירות DNS. שרת DNS עצמו חייב להיות מוגדר עם כתובת IP קבועה. בנוסף, עליך להגדיר את מאפייני TCP/IP, כך שהגדרות DNS יצביעו חזרה לשרת. תוכל להתקין את שירות DNS בכל עת, בזמן או לאחר התקנת Windows 2000 Server.

תהליך התקנת DNS מבצע את הפעולות הבאות:

- ❖ מתקין את תוסף התוכנה של DNS ומוסיף קיצור דרך עבורו בתיקיה Administrative Tools שבתפריט Programs של התפריט הראשי Start.
- ❖ מוסיף את מפתח שירות DNS הבא לרישום המערכת:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DNS

- ❖ יוצר את התיקיה %systemroot%\System32\DNS אשר מכילה את קבצי מסד הנתונים של DNS.

בדרך כלל לא תצטרך לערוך את קבצי מסד הנתונים של DNS. אולם, תוכל להיעזר בהם כדי לפתור תקלה הקשורה ב-DNS. שירות DNS מספק מספר קבצים לדוגמה, הנמצאים בתיקיה %systemroot%\System32\DNS\Samples, לאחר התקנת השירות.

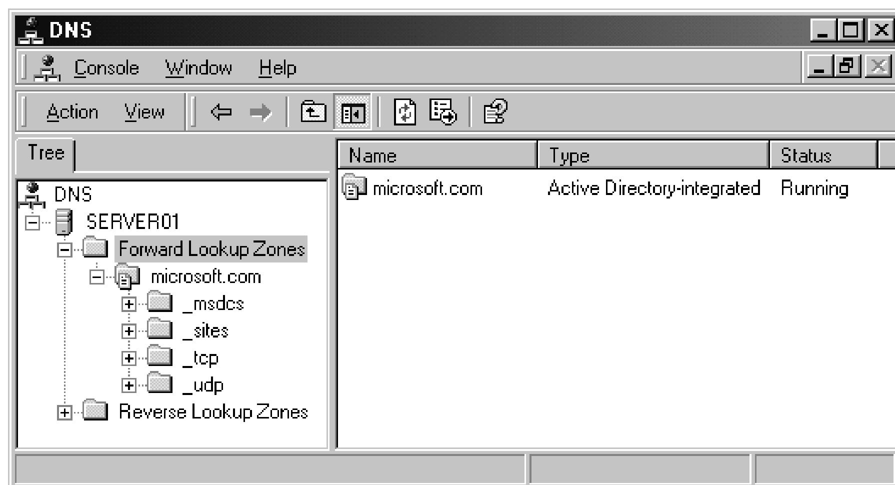
הערה התיקיה %systemroot%\System32\DNS\Samples **כוללת את הקובץ** BOOT. **קובץ זה אינו** מוזכר בקובץ RFC **ואינו** נדרש לצורך עמידה בדרישות RFC. אבל, הקובץ BOOT **הוא** חלק מ-BIND (**B**erkeley **I**nternet **N**aming **D**aemon) - **יישום ספציפי** של DNS. אם אתה משדרג משרת DNS של BIND, העתקת הקובץ BOOT תאפשר לך הגירה (Migration) קלה של התצורה הקיימת.

הגדרת שירות DNS

לאחר שהשירות מותקן אתה מוכן להגדיר ולנהל אותו.

תוסף התוכנה של DNS

תוכל להשתמש בתוסף התוכנה של DNS, כמו זה המוצג בתרשים 9.13, לכל משימות הניהול וההגדרה של DNS. תוסף התוכנה של DNS יאפשר לך להגדיר אזורים לביצוע שאילתות לפנים ולאחור (Forward Lookup Zones ו-Reverse Lookup Zones), להוסיף רשומות משאבים (RR-Resorce Records) לקובץ מסד הנתונים של האזור ולהגדיר את DNS עבור Dynamic DNS (DDNS), מה שיאפשר עדכון אוטומטי של קבצי מסד נתוני האזור שלך עם שרתים או שירותים אחרים.



תרשים 9.13 תוסף התוכנה של DNS.

תוכל לגשת אל תוסף התוכנה של DNS כ-MMC Console נפרד, או דרך תוסף התוכנה של Computer Management שתחת Services and Applications. תוסף התוכנה של DNS יכול להיות מותקן על ידי הפעלת Adminpak.msi, או על ידי התקנת שירות DNS. לפני ששירות DNS מותקן, יכול תוסף התוכנה של DNS לשמש עבור ניהול שרתים מרוחקים בהם פועל שירות DNS.

Forward Lookup Zone

אזור חיפוש לפנים (Forward Lookup Zone) מאפשר ביצוע שאילתות לחיפוש לפנים. בשרתי שמות עליך להגדיר לפחות אזור חיפוש לפנים אחד כדי ששירות DNS יפעל.

כדי ליצור אזור חיפוש לפנים חדש, בחר בתיקיה Forward Lookup Zone, פתח את תפריט Action וממנו בחר New Zone. האשף New Zone מנחה אותך בנבכי תהליך יצירת אזור חיפוש לפנים חדש. באמצעות האשף ניתן להגדיר את האפשרויות הבאות:

Zone Type

קיימים שלושה סוגי אזור (Zone Type) אותם ניתן להגדיר:

- **Active Directory-integrated** – אזור מסוג זה, המשולב ב-Active Directory, הוא העתק ראשי (Master Copy) של אזור חדש. האזור משתמש בשירותי Active Directory כדי לאחסן ולשכפל קבצי אזור. בדרך זו מתאפשר עדכון מאובטח ואחסון משולב. באזור משולב Active Directory לא מתבצעות העברות אזור תקניות (Zone Transfer). במקום זאת, קובץ מסד הנתונים של האזור משוכפל (Replicate) כחלק משכפול Active Directory Store.
- **Standard Primary** – אזור תקני ראשי מחזיק העתק ראשי של אזור חדש והוא מאוחסן בקובץ טקסט תקני. אתה מנהל ומתחזק אזור ראשי במחשב בו נוצר האזור. אפשרות זו מקלה על חילופי נתוני DNS עם שרתי DNS אחרים, המשתמשים בשיטות אחסון מבוססות טקסט.
- **Standard Secondary** – אזור תקני משני הוא שיעתוק (העתק משוכפל) של אזור קיים (ראשי או משני). אזורים משניים מוגדרים לקריאה בלבד ומאוחסנים בקבצי טקסט רגילים. כדי שניתן יהיה ליצור אזור משני, חייב להיות מוגדר אזור ראשי. בעת יצירת אזור משני, עליך לציין את שרת DNS, הנקרא Master Server, אשר מעביר נתוני אזור לשרת השמות המכיל את האזור התקני המשני. יצירת האזור המשני נועדה לספק יתירות (Redundancy) וכדי להפחית את העומס המוטל על שרת השמות, המכיל את קובץ מסד נתוני האזור הראשי.

Zone Name

בדרך כלל, נקרא האזור על פי שמו של ה-domain הגבוה ביותר בהיררכיה הכלולה באזור, כלומר, ה-Root Domain של האזור. לדוגמה, לאזור המכיל את ה-Domains: microsoft.com ו- sales.microsoft.com, שם האזור (Zone Name) יהיה microsoft.com.

Zone File

קובץ אזור (Zone File) מתייחס לקובץ מסד נתוני האזור, אשר סיומת ברירת המחדל שלו היא dns. לדוגמה, אם שם האזור (Zone Name) הוא microsoft.com, יהיה שם ברירת המחדל לקובץ מסד נתוני האזור microsoft.com.dns.

כאשר מניידים (Migrating) אזור משרת אחר ניתן לייבא קובץ אזור קיים. עליך להציב את הקובץ הקיים בתיקיה systemroot%\System32\DNS% במחשב היעד לפני שאתה יוצר אזור חדש.

Zone Transfer

קיימות שתי שיטות להעברת אזור:

- Full-Zone Transfer - AXFR (העברת אזור מלא)
- Incremental Zone Transfer - IXFR (העברת אזור חלקית)

AXFR היא הדרך התקנית להעברת נתוני אזור, והיא בעיקרה העתקה של קובץ האזור. Windows 2000 תומכת ב-AXFR, אך היא תומכת גם ב-IXFR, המנצל רוחב פס צר יותר מכיון שבשיטה זו מועברים רק השינויים באזור.

Reverse Lookup Zone

אזור חיפוש לאחור (Reverse Lookup Zone) מאפשר ביצוען של שאילתות חיפוש לאחור. אזורי חיפוש לאחור אינם חובה, אולם, הם דרושים לצורך הפעלת כלי תמיכה ואיתור תקלות, כגון nslookup, וכדי לרשום שם במקום כתובת IP בקבצי היומן של שירותי IIS (**I**nternet **I**nformation **S**ervices Log Files).

כדי ליצור אזור חיפוש לאחור חדש בחר בתיקיה Reverse Lookup Zone, פתח את תפריט Action ובחר New Zone. אשף New Zone ינחה אותך בנבכי תהליך יצירת אזור חיפוש לאחור חדש. באמצעות האשף ניתן להגדיר את האפשרויות הבאות:

Zone Type

סוגי האזור (Zone Types) במקרה זה זהים לאלו הזמינים בעת יצירת אזור חיפוש לפנים (Forward Lookup Zone):

- Active Directory-integrated,
- Standard Primary,
- Standard Secondary.

Reverse Lookup Zone

הקלד את זיהוי הרשת שלך, או את שם אזור החיפוש לאחור. אם אתה משתמש בערך 0 (אפס) בזיהוי הרשת שלך, הוא יופיע גם בשם האזור. לדוגמה, זיהוי רשת (Network ID) 192 יצור את האזור in-addr.arpa .192 ואילו זיהוי רשת 192.0 יצור את האזור 0.192.in-addr.arpa.

Zone File

שם ברירת המחדל של קובץ האזור נקבע על פי זיהוי הרשת ו-Subnet Mask. DNS הופכת את סדר האוקטטים ומוסיפה להם את הסיומת in-addr.arpa. לדוגמה, אזור חיפוש לאחור של רשת 192.254 יהפוך להיות 254.192.in-addr.arpa.dns.

כאשר מניידים אזור משרת אחר תוכל לייבא קובץ אזור קיים. עליך להציב את הקובץ הקיים בתיקיה systemroot%\System32\DNS% במחשב היעד, לפני שאתה יוצר אזור חדש.

Resource Records

לאחר שיצרת את האזורים שלך תוכל להיעזר בתוסף התוכנה של DNS כדי להוסיף רשומות משאבים. רשומות משאבים (Resource Records) הן רשומות בקובץ מסד הנתונים של האזור (Zone File). כל רשומת משאב מזהה משאב מסוים במסד הנתונים. כדי להוסיף רשומת משאב, בחר באזור אליו אתה מעוניין להוסיף את המשאב, פתח את תפריט Action וממנו בחר Other New Record. כאשר מופיעה תיבת הדו-שיח Resource Record Type תוכל ליצור רשומות לכל סוגי הרשומות המופיעים ברשימה הנפתחת Select A Resource Record Type.

קיימים סוגים רבים של רשומות משאבים. כאשר נוצר אזור, מוסיף DNS באופן אוטומטי שתי רשומות משאב: SOA (**S**tart **O**f **A**uthority) ו- NS (**N**ame **S**erver). רשומת SOA מזהה איזה שרת שמות (Name Server) הוא מקור הנתונים המוסמך לפתור שמות ב-Domain. הרשומה הראשונה בקובץ מסד נתוני אזור חייבת להיות רשומת SOA. רשומת NS מכילה את שמות שרתי השמות המשויכים ל-Domain מסוים. שני סוגי רשומות אלה יכולים להיות מוגדרים בתיבת הדו-שיח Properties של אזור החיפוש לפנים הרצוי.

לרשימה של יתר סוגי רשומות המשאבים, כולל תיאור של כל סוג וסוג, פתח את תיבת הדו-שיח Resource Record Type ובחן את כל הסוגים המופיעים ברשימה Select a resource record type. כשאתה בוחר בסוג רשומה מופיע בתחתית תיבת הדו-שיח תיאור שלו.

הערה למידע נוסף אודות רשומות משאבים, קרא את קבצי RFC 1034, RFC 2052 ואת RFC 2065. למידע נוסף לגבי אופן פעולתו של DNS, קרא את הספר *DNS and BIND* מאת *Paul Albitz* ו- *Cricket Liu*, בהוצאת *O'Reilly and Associates, Inc.* (1998).

Dynamic DNS

שירות DNS כולל אפשרות לעדכון דינמי הנקראת Dynamic DNS, או בקיצור DDNS. כאשר מתרחשים שינויים ב-Domain בו פועל שרת DNS רגיל, עליך לעדכן באופן ידני את קובץ מסד נתוני האזור בשרת השמות הראשי. עם DDNS שרתי השמות והלקוחות ברשת מעדכנים את קבצי מסד נתוני האזור באופן אוטומטי.

עדכונים דינמיים

תוכל להגדיר רשימה של שרתים מוסמכים שיזמו עדכונים דינמיים. רשימה זו יכולה לכלול Secondary Name Servers, DCs ומחשבים נוספים המספקים שירותי רישום ללקוחות ברשת, כגון שרתי DHCP או WINS.

רצף העדכון כולל את הצעדים הבאים:

1. לקוח, הנעזר בשאילתת SOA, מאתר את שרת DNS הראשי ומוסמך אזור (Zone Authoritative), עבור הרשומה אותה יש לרשום.
2. הלקוח שולח לשרת ה-DNS עדכון החלטי או עדכון שנקבע מראש עבורו בלבד, כדי לוודא קיומו של רישום. אם הרישום אינו קיים, שולח הלקוח את חבילת העדכון הדינמי המתאימה לרישום הרשומה.
3. אם העדכון נכשל, מנסה הלקוח לרשום את הרשומה בשרת DNS ראשי אחר, אם האזור המוסמך הוא Multimaster. אם כל שרתי DNS נכשלים בביצוע העדכון הדינמי, מתרחש התהליך שוב לאחר 5 דקות, ואם הוא נכשל שוב הוא יתבצע לאחר 10 דקות. אם הרישום עדיין נכשל, מתבצע התהליך המתואר 50 דקות לאחר הניסיון האחרון.

כל מחשב הפועל בסביבת Windows 2000 מנסה לבצע רישום של רשומות מסוג A ו-PTR שלו. רשומת A, ידועה גם בשמה כרשומת מארח (Host Record), מספקת מיפוי שם-לכתובת (Name-to-Address Mapping), ואילו רשומת PTR, הידועה גם כרשומת מצביע (Pointer Record), מספקת מיפוי כתובת-לשם (Address-to-Name Mapping) עבור המחשב השולח את הרישום. השירות אשר מחולל למעשה את העדכונים הדינמיים של DNS הוא שירות DHCP. שירות DHCP פועל בכל מחשב Windows 2000, ללא קשר אם הוא מוגדר כלקוח DHCP או לא.

DDNS ו-DHCP

DDNS פועל בהדדיות עם שירות DHCP, כדי לשמר את סנכרון מיפוי שמות-לכתובות IP בין מארחי הרשת. כברירת מחדל, שירות DHCP מאפשר ללקוחות להוסיף את רשומת A (Host) שלהם ל-Zone, והשירות DHCP עצמו מוסיף את רשומת PTR (Pointer) של הלקוח ל-Zone. שירות DHCP מנקה את שתי הרשומות כאשר פג תוקף חוזה החכירה.

כדי להגדיר Zone כדינמי היעזר בתוסף התוכנה של DNS. בחר באזור הרצוי, פתח את תפריט Action ובחר Properties. בכרטיסיה General של תיבת הדו-שיח Properties, פתח את הרשימה Allow Dynamic Updates ובחר באפשרות Yes.

כדי להגדיר את שרת DHCP, כך שישלח עדכונים דינמיים, היעזר בתוסף התוכנה של DHCP להגדרת שרת DHCP, כך שיצביע לכיוון שרתי DNS המתאימים.

הערה למידע נוסף אודות Dynamic DNS קרא את RFC 2136 ואת RFC 2137. היעזר בדפדפן האינטרנט שלך כדי לחפש אחר הערכים "RFC 2136" ו-"RFC 2137".

מידע נוסף אודות DDNS ויישומו תוכל למצוא בתקליטור המצורף לספר זה (\chapt09\articles\w2kDNS.doc).

תרגיל 4: הגדרת שירות DNS

בתרגיל זה תמחק ותיצור מחדש אזור חיפוש לפנים, תיצור אזור חיפוש לאחור, תגדיר Dynamic DNS ותבחן את שרת DNS שלך. להשלמת תרגיל זה תשתמש בשרתים Server01 ו-Server02.

הערה בפרק 6, תרגיל 1 "התקנת Active Directory Services", הותקן DNS באופן אוטומטי, מפני ש-Server01, כשרת העומד בפני עצמו, לא נעזר ב-DNS להסדרה והמרה של שמות. התקנת DNS דומה להתקנת DHCP ו-WINS - DNS הוא רכיב של שירותי הרשת (Network Services). אם אתה מעוניין, נווט לפרטי Network Services כדי לבחון אם DNS אכן מותקן.

הליך 1: אזור חיפוש לפנים ויצירת אזור חיפוש לאחור

בהליך זה, תמחק את סוג האזור Active Directory-integrated שנוצר כתוצאה מהתקנת DNS. אז, תיצור אזורי חיפוש רגילים לפנים ולאחור.

1. היכנס ל-Server01 בשם משתמש Administrator ועם הסיסמה password.
2. לחץ Start, הצבע על Programs, הצבע על Administrative Tools ובחר DNS.

   תוסף התוכנה של DNS יופיע.
3. מזער את תוסף התוכנה של DNS.
4. בחלון Tree, הרחב את SERVER01 והרחב את התיקיה Forward Lookup Zones.
5. בחר במכולה microsoft.com.
6. פתח את תפריט Action והקש על Delete.
7. תופיע הודעה השואלת אם אתה בטוח שאתה מעוניין למחוק. לחץ OK.

   תופיע הודעת אזהרה של DNS.

8. קרא את הודעת האזהרה המופיעה ולחץ Yes.

9. פתח את תפריט Action ולחץ על New Zone. האשף New Zone יופיע.

10. לחץ Next. יופיע החלון Zone Type.

11. ודא כי לחצן האפשרויות Standard Primary נבחר, ולחץ Next. יופיע החלון Zone Name.

12. הקלד microsoft.com ולחץ Next.

13. יופיע החלון Zone File.

14. ודא כי לחצן האפשרויות Create A New File With This File Name נבחר, וכי שם הקובץ שנוצר הוא microsoft.com.dns.

15. לחץ Next. יופיע החלון Completing The New Zone Wizard.

16. סקור את הנתונים המופיעים בחלון זה, ולסיום לחץ על Finish.

    תוסף התוכנה של DNS יופיע.

17. בחלון Tree לחץ על microsoft.com. שים לב שהרשומות SOA (Start Of Authority) , NS (Name Server) ו- HOST - A נוצרות.

    Server01 מסוגל כעת להסדיר (להמיר) שמות מארחים לכתובות IP, תוך שימוש בקובץ אזור החיפוש Standard Primary.

18. בחלון Tree, לחץ על המכולה Reverse Lookup Zones.

19. פתח את תפריט Action ולחץ על New Zone. האשף New Zone יופיע.

20. לחץ Next. יופיע החלון Zone Type.

21. ודא כי לחצן האפשרויות Standard Primary נבחר, ולחץ Next.

    יופיע החלון Reverse Lookup Zone.

22. ודא כי הלחצן Network ID נבחר, והקלד 192.168.1 בתיבה Network ID.

    תיבת הטקסט Reverse Lookup Zone Name שבתחתית המסך מכילה כעת את הערך 1.168.192.in-addr.arpa.

23. לחץ Next. יופיע החלון Zone File.

24. ודא כי לחצן האפשרויות Create A New File With This File Name נבחר וכי שם הקובץ שייווצר הוא 1.168.192.in-addr.arpa.dns.

25. לחץ Next. מופיע החלון Completing The New Zone Wizard.

26. סקור את הנתונים המופיעים בחלון זה, ולסיום לחץ על Finish.

כעת, כאשר הוא מקבל כתובת של מארח ברשת המשנה שלו, מסוגל שירות DNS ב-Server01 לספק את שמות המארחים.

הערה לאחר יצירת DNS, בדרך כלל מתוספים נתוני הגדרת DNS לשירות DHCP. השלמת את ההליך לעיל בתרגול DHCP, אותו ביצעת קודם לכן בפרק זה.

הליך 2: הגדרת שירות DNS דינמי

בהליך זה תגדיר את שירות DNS לאפשר עדכונים דינמיים. השלם הליך זה תוך שימוש בתוסף התוכנה של DNS ב-Server01.

1. בחלון Tree, בחר במכולה microsoft.com. תיקיה זו היא תיקיית משנה של התיקיה Forward Lookup Zones.
2. פתח את תפריט Action ולחץ על Properties.

   תיבת הדו-שיח microsoft.com Properties תופיע.
3. מתיבת הרשימה Allow Dynamic Updates בחר Yes ולחץ OK.

   חלק זה של ההליך הגדיר DNS דינמי עבור אזור החיפוש לפנים.
4. בחלון Tree, בחר במכולה 192.168.1.x Subnet.
5. פתח את תפריט Action ובחר Properties.

   תיבת הדו-שיח 192.168.1.x Subnet Properties תופיע.
6. מתיבת הרשימה Allow Dynamic Updates בחר Yes ולחץ OK.

   חלק זה של ההליך הגדיר DNS דינמי עבור אזור החיפוש לאחור.
7. מזער את תוסף התוכנה של DNS.

הליך 3: בחינה והגדרה נוספת של DNS

בהליך זה תוודא כי שירות DNS פועל כשורה ותמשיך להגדיר את DNS, תוך שימוש בתוסף התוכנה של DNS.

1. ב-Server01 שחזר את חלון תוסף התוכנה של DNS הממוזער.
2. בחלון Tree, לחץ על SERVER01.
3. פתח את תפריט Action ובחר Properties. תיבת הדו-שיח SERVER01 Properties תופיע.
4. בחר בכרטיסיה Monitoring.
5. באזור Select A Test Type סמן את A Simple Query Against This DNS Server ואת A Recursive Query To Other DNS Servers.
6. לחץ על Test Now. בתיבה Test Results עליך לראות את הערך PASS מופיע בשני הטורים. אם אתה בשרת העומד בפני עצמו יופיע בעמודה Recursive Query הערך FAIL.
7. לחץ OK. תוסף התוכנה של DNS יופיע.
8. בחלון Tree לחץ על Reverse Lookup Zones.
9. לחץ על 192.168.1.x Subnet.

   שים לב בחלונית הפרטים, שאזור החיפוש לאחור (Reverse Lookup Zone) כולל שתי רשומות: SOA ו-NS.
10. בחלון Tree לחץ על 192.168.1.x Subnet.
11. פתח את תפריט Action ובחר New Pointer. תיבת הדו-שיח New Resource Record תופיע.
12. בתיבה Host IP Number, באוקטט הנבחר, הקלד **201**.
13. בתיבה Host Name הקלד **server01.microsoft.com.** (ודא כי הנקודה אחרי המחרוזת com אכן הוקלדה).
14. לחץ OK. רשומת Pointer מופיעה בחלונית הפרטים.
15. סגור את תוסף התוכנה של DNS.
16. פתח חלון שורת פקודה (Command Prompt) ב-Server01 או ב-Server02.

17. בשורת הפקודה הקלד **nslookup** והקש Enter.

מ-Server01, מוגדר שרת ברירת המחדל כ- localhost וכתובת ה-IP הרשומה לו היא 127.0.0.1.

מ-Server02, מוגדר שרת ברירת המחדל כ- server01.microsoft.com וכתובת ה-IP הרשומה לו היא 192.168.1.201.

שני הרישומים מצביעים לעברו של server01.microsoft.com. הרישום המופיע בשורת הפקודה שב-Server01 הוא של כתובת הלולאה הפנימית שלו.

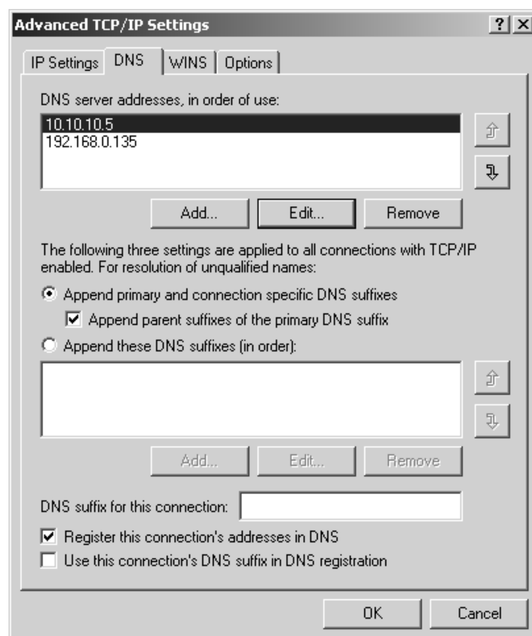
18. הקלד **ls.microsoft.com**.

שים לב שהרשומות NS ו-A מוצגות כתוצאה משאילתת DNS זו.

19. הקלד **Exit** והקש Enter. סגור את חלון שורת הפקודה.

הגדרת לקוח DNS

לאחר שתתקין ותגדיר את שירות DNS במחשב הפועל בסביבת Windows 2000 Server, תוכל להגדיר את לקוחות DNS של Windows 2000 שלך. לפני שתוכל להגדיר את הלקוח לשימוש בשירות DNS, עליך להבטיח כי פרוטוקול TCP/IP מותקן בו. לאחר שפרוטוקול TCP/IP מותקן בלקוח, פתח את תיבת הדו-שיח Internet Protocol (TCP/IP) Properties (ראה תרשים 9.4). מכאן תוכל להגדיר קבלת כתובת DNS אוטומטית (מסופק על ידי שרת DHCP), או לקבוע את כתובות ה-IP של שרת DNS מועדף ושרת DNS משני. ניתן להגדיר אפשרויות מתקדמות עוד יותר עבור DNS, על ידי לחיצה על לחצן Advanced לפני הגדרת שרתי DNS. מתיבת הדו-שיח Advanced TCP/IP Settings (תרשים 9.14) בחר בכרטיסיה DNS והגדר את DNS. יהיה עליך לציין כתובת, או כתובות, עבור שרתי DNS. יש לרשום אותם על פי סדר השימוש בהם. בתיבת דו-שיח זו תוכל גם להגדיר הגדרות DNS, המסייעות בפתרון שמות שלא צוינו באמצעות FQDN (Fully Qualified Domain Name) שלהם, ותוכל להגדיר הגדרות רישום DDNS.



תרשים 9.14 תיבת הדו-שיח Advanced TCP/IP Settings מראה שתי כתובות DNS, המסודרות על פי סדר השימוש בהן, מאפייני פתרון שמות והגדרות לרישום אוטומטי.

איתור תקלות בשירות DNS

ניתן לאתר תקלות בשרתי שמות באמצעות אפשרויות הניטור ורישומי היומן של תוסף התוכנה של DNS, או תוך שימוש בתוכנית השירות nslookup, המופעלת משורת הפקודה.

ניטור שירות DNS

תוסף התוכנה של DNS מאפשר ניטור של שירות DNS. בחר בשרת השמות, פתח את תפריט Action ובחר Properties. בתיבת הדו-שיח Properties של השרת הנבחר בחר בכרטיסיה Monitoring. באפשרותך לבחון את שרת השמות על ידי ביצוע שני סוגי שאילתה:

- **Simple Query** (שאילתה פשוטה) – בחר באפשרות זו כדי לבדוק את שרת DNS באמצעות שאילתה פשוטה. זוהי בדיקה מקומית אשר עושה שימוש בלקוח DNS במחשב הזה, כדי לבדוק את שרת השמות (Name Server).
- **Recursive Query** (שאילתה רקורסיבית) – בחר בסוג זה של שאילתה כדי לבצע בדיקה מורכבת יותר של שרת השמות. שאילתה זו בודקת את שרת השמות, על ידי כך שהיא שולחת שאילתה רקורסיבית לשרת שמות אחר.

Logging

תוסף התוכנה של DNS מאפשר לך גם לקבוע אפשרויות נוספות לרישומי יומנים, לצורך ניפוי שגיאות (Debugging). פתח את תיבת הדו-שיח Properties של שרת השמות ובחר בכרטיסיה Logging. כאן תוכל לבחור מתוך 11 אפשרויות העומדות בפניך: Full Packets ,TCP ,UDP ,Receive ,Send ,Answers ,Questions ,Update ,Notify ,Query ו- Write Through. נתונים של כל אחת מאפשרויות אלו נשמרים לקובץ יומן (Log file).

Nslookup

תוכנית השירות של שורת הפקודה nslookup היא כלי האבחון העיקרי של שירות DNS והיא מותקנת בעת שמותקן פרוטוקול TCP/IP. היעזר ב-nslookup כדי לצפות ברשומות משאבים וכדי לכוון שאילתות לכל שרת שמות, כולל יישומי DNS במערכות UNIX.

ל-nslookup יש שני מצבים:

- Interactive,
- NonInteractive.

כשדרושה לך יותר מאשר פיסת נתונים בודדת, השתמש באפשרות ההפעלה האינטראקטיבית. כדי להפעיל את nslookup במצב אינטראקטיבי הקלד **nslookup** בשורת הפקודה והקש Enter. כדי לצאת ממצב זה הקש exit.

כשדרושה לך פיסת נתונים בודדת, השתמש באפשרות ההפעלה הלא-אינטראקטיבית. הקלד בשורת הפקודה את פקודת nslookup עם פרמטרים מדויקים לגבי הנתונים הנדרשים לך. מבנה פקודה נכון של nslookup נראה כך:

```
nslookup [-options...] [computer-to-find | - [server]]
```

הטבלה הבאה מסבירה את הפרמטרים של nslookup.

מבנה פקודה	תיאור
-options...	מגדיר פקודת nslookup אחת או יותר. לרשימת הפקודות הקלד סימן שאלה במצב אינטראקטיבי כדי לפתוח את מערכת העזרה.
computer-to-find	אם ה"מחשב-לאיתור" הוא כתובת IP, nslookup תשיב בשם המחשב המארח. אם ה"מחשב-לאיתור" הוא שם מחשב מארח, nslookup תשיב בכתובת IP. אם ה"מחשב-לאיתור" הוא שם ואין בו נקודה עוקבת, מתוסף לשם גם שם ברירת המחדל של DNS Domain. כדי לאתר מחשב הנמצא מחוץ ל-DNS Domain הנוכחי הוסף בסוף השם גם נקודה.
server	השתמש בשרת זה כ-DNS Domain Server. אם פרמטר זה אינו נכלל בפקודה, ישמש לצורך זה השרת המוגדר כשרת שמות ברירת המחדל הנוכחי.

סיכום שיעור

DNS הוא מסד נתונים מבוזר, המשמש ברשתות TCP/IP לצורך תרגום שמות מחשבים לכתובות IP שלהם. Domain namespace היא שיטת מתן שמות המספקת את המבנה ההיררכי עבור מסד נתוני DNS. המבנה ההיררכי של Domain Namespace בנוי מתחומי שורש (Root Domain), תחומים ברמה עליונה (Top-Level Domain), תחומים ברמה משנית (Second-Level Domain) ושמות מארחים (Host Name). אזורים (Zones) מספקים דרך לחלוקת Domain namespace למחיצות קלות לניהול. אזור חייב לכלול רצף אחיד מה-Domain namespace. שרת שמות DNS מאחסן את קובץ מסד נתוני האזור ויכול להיות בעל סמכות ביותר מאשר רק אזור בודד. פתרון שמות (Name Resolution) היא תהליך המרת שם המחשב לכתובת IP. שאילתת חיפוש לאחור (Reverse Lookup Query) ממירה כתובת IP לשם. כדי ליישם DNS, עליך להתקין את שירות DNS ולהגדיר את השרת לשימוש בתוסף התוכנה של DNS. תוכל להיעזר בתוסף התוכנה של DNS להגדרת אזורי חיפוש לפנים (Forward Lookup Zones) ואזורי חיפוש לאחור (Reverse Lookup Zones), להוספת רשומות משאבים לקובץ מסד נתוני האזור, ולהגדיר את שירות DNS לצורך DDNS, מה שיאפשר עדכון אוטומטי של קבצי האזור שלך על ידי שרתים או שירותים אחרים. בנוסף להגדרת DNS במחשב שרת Windows 2000 עליך להגדיר גם את לקוח Windows 2000. כדי להגדיר לקוח DNS חייב להיות מותקן במחשב זה פרוטוקול TCP/IP, ובתיבת הדו-שיח Internet Protocol (TCP/IP) Properties חייבות להיות הגדרות DNS תקינות ותואמות. לאחר ש-DNS מותקן ברשת שלך, תוכל לאבחן את שירות DNS באמצעות כלי הניטור ורישומי היומן, שהם חלק מתוסף התוכנה של DNS, או תוך שימוש בתוכנית השירות nslookup.

שאלות סיכום

השאלות הבאות נועדו לחזק מידע מפתח שהוצג בפרק זה. אם אינך מסוגל לענות על שאלה סקור את השיעור המתאים ונסה לענות על השאלה פעם נוספת. תשובות לשאלות תמצא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

1. Your computer receives its TCP/ IP configuration information from a DHCP server in the network. After DHCP information is received, you can connect to any host on your own subnet, but you cannot connect to or successfully ping any host on a remote subnet. You checked the DHCP Service to ensure that the router information specified for your address scope is correct. What is the likely cause of the problem and how would you fix it?
2. You installed NWLink IPX/ SPX and GSNW. After installing these components, you cannot communicate with one of the NetWare servers on your network. You have no trouble accessing this NetWare server from your client computer running Windows 2000 Professional, NWLink IPX/ SPX, and CSNW. You must communicate with this NetWare server from your Windows 2000 Server because the NetWare server contains resources you must make available to users running the Microsoft Network Client. What is the likely cause of the problem?
3. You notice that access to network resources seems slower on your computer running Windows 2000 Server than from another identical computer running Windows 2000 Server on the same network. The only difference you can determine is that the slower Windows 2000 Server computer is running multiple protocols. How could network protocol binding order potentially resolve this problem?
4. When do DHCP clients attempt to renew their leases?
5. Why might you create multiple scopes on a DHCP server?
6. How can you manually restore the DHCP database?
7. What are the configuration requirements for a WINS server?
8. Why would you want to have multiple name servers?
9. Why do you create forward and reverse lookup zones?
10. What is the difference between Dynamic DNS and DNS?

1. המחשב שלך מקבל את נתוני תצורת TCP/IP שלו משרת DHCP ברשת. לאחר שנתוני DHCP מתקבלים, אתה יכול להתחבר לכל מחשב מארח ברשת המקומית שלך, אך אינך מצליח להתחבר או לבצע PING מוצלח עם מחשב כלשהו ברשת משנה אחרת. בדקת את שירות DHCP כדי לוודא שנתוני הנתב המוגדרים עבור מרחב הכתובות שלך נכונים. מהו הגורם הסביר לתקלה וכיצד עליך לפתור אותה?

2. התקנת את NWLink IPX/SPX ואת GSNW. לאחר התקנת רכיבים אלה אינך מצליח לתקשר עם אחד משרתי NetWare ברשת שלך. אין לך כל בעיה לגשת לשרת NetWare זה ממחשב לקוח הפועל בסביבת Windows 2000 Professional עם NWLink IPX/SPX ו-CSNW. אתה חייב לתקשר עם שרת NetWare שלך מתוך שרת Windows 2000, מפני ששרת NetWare מכיל משאבים שאתה חייב שיהיו זמינים למשתמשים המפעילים את Microsoft Network Client. מה יכולה להיות הסיבה לתקלה?

3. אתה מבחין כי הגישה למשאבי רשת הפכה לאיטית בשרת Windows 2000 שלך, יותר משהיא בשרתי Windows 2000 אחרים זהים באותה רשת. ההבדל היחידי שאתה יכול להבחין בו הוא ששרת Windows 2000 האיטי יותר מפעיל מספר פרוטוקולי תקשורת. כיצד יכול סדר כריכת פרוטוקולי התקשורת לסייע בפתרון הבעיה?

4. מתי מנסים לקוחות DHCP לחדש את החוזים שלהם?

5. מדוע ייתכן שתרצה ליצור יותר מאשר מרחב (Scope) אחד בשרת DHCP?

6. כיצד ניתן לשחזר באופן ידני את מסד נתוני DHCP?

7. מהן דרישות התצורה של שרת WINS?

8. מדוע רצוי שיהיו לך מספר שרתי שמות (Name Server)?

9. מדוע עליך ליצור אזורי חיפוש לאחור ולפנים?

10. מה ההבדל בין DNS לבין Dynamic DNS?

פרק 10

שירות ניתוב וגישה מרחוק (RRAS)

אודות פרק זה

שירות ניתוב וגישה מרחוק (**R**outing and **R**emote **A**ccess **S**ervice - RRAS) משלב שירותי שרת לניתוב מרובה פרוטוקולים ורישות פרטי וירטואלי (Virtual Private Network) בשרתי Windows 2000. השירות הוצג לראשונה בשרתי Windows NT 4.0 ונועד לספק שירותים ורכיבים להפיכת המחשב לנתב ביניים דינמי לתוכנה (Mid-range Dynamic Software Router). פרק זה מציג בפניך את אופן יישום RRAS בסביבת Windows 2000. הפרק דן גם במאפייני השירות, כיצד מיושמת הגישה מרחוק ורישות פרטי וירטואלי, וכן בכלים הזמינים ב-Windows 2000 לניהול RRAS.

לפני שתתחיל

לביצוע השיעורים בפרק זה נדרש :

- ❖ Server01 ו-Server02 ובהם מותקן ופועל שרת Microsoft Windows 2000.
- ❖ ב-Server01 מודם מותקן ומוגדר כהלכה. ייתכן שהתקנת שרת Windows 2000 זיהתה באופן אוטומטי את המודם המותקן במחשב. אם לא, השתמש ביישומון Add/Remove Hardware שבלוח הבקרה (Control Panel), כדי להתקין את מנהלי ההתקן התואמים לתמיכה במודם שלך.
- ❖ השלמת כל התרגילים בפרקים קודמים.

הערה: אין צורך במדפסת כדי להשלים את התרגילים בפרק זה.

שיעור 1: מבוא לשירות ניתוב וגישה מרחוק

התמיכה בניתוב מרובה פרוטוקולים במשפחת מערכות ההפעלה Windows NT החל בגירסה 3.51, בה הותקנה חבילת השירות 2 (Service Pack 2). חבילת השירות כללה רכיבי RIP (**R**outing **I**nformarion **P**rotocol) עבור IP, RIP עבור IPX ו-SAP (Service Advertising Protocol) עבור IPX. Windows NT 4.0 כוללת גם היא את הרכיבים הללו. בחודש יוני של 1996 הפיצה Microsoft את RRAS ל- Windows NT 4.0. רכיב זה החליף את שירות הגישה מרחוק (RAS) של Windows NT 4.0 ואת שירותי RIP עבור IP, RIP עבור IPX ו-SAP עבור IPX, בשירות משולב יחיד, המספק גם גישה מרחוק וגם ניתוב מרובה פרוטוקולים. שיעור זה מתמקד באופן יישום RRAS ב-Windows 2000. הוא דן בהתקנה והגדרה, כמו גם באישורים והרשאות.

לאחר שיעור זה, תוכל

- לתאר את RRAS ב-Windows 2000
- להשתמש בתוסף התוכנה של Routing And Remote Access, כדי להגדיר ולאפשר RRAS.

זמן לימוד משוער: 30 דקות

Windows 2000 RRAS

RRAS (**R**outing and **R**emote **A**ccess **S**ervice) של שרת Windows 2000 ממשיך את התפתחות שירותי הניתוב מרובה הפרוטוקולים והגישה מרחוק עבור פלטפורמת Windows. כאשר יושם RRAS בסביבת Windows NT 4.0 הוא הוסיף תמיכה בתכונות הבאות:

- גירסה 2 של RIP עבור IP (גירסה 1 של RIP עבור IP עדיין נתמכת).
- פרוטוקול ניתוב OSPF (**O**pen **S**hortest **P**ath **F**irst) עבור IP.
- ניתוב חיוג על-פי דרישה - Demand-Dial Routing (ניתוב על קישורי WAN קבועים או על-פי דרישה, כגון באמצעות קווי טלפון אנלוגיים).
- גילוי נתב ICMP (**I**nternet **C**ontrol **M**essage **P**rotocol).
- לקוח RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice), לניצול יתרונות השירותים המסופקים על ידי RADIUS.
- שרת RADIUS, לריכוז אימות (Authentication), הרשאה (Authorization), ניהול חשבונות משתמשים (Accounting) ומדיניות גישה מרחוק (Remote Access Policy) ללקוחות בגישה מרחוק לרשת VPN וללקוחות התקשרות בחיוג (Dial-in, צורף ל-Option Pack עבור Windows NT 4.0).

- סינון מנות IP ו-IPX לאבטחת מידע ברמת הפרוטוקול.
- תוכנית ניהול בעלת ממשק משתמש גרפי (GUI) בשם Routing and RAS Admin, ותוכנית שירות המופעלת משורת הפקודה בשם Routemon.

ב-Windows 2000 נוספו ל-RRAS המאפיינים הבאים:

- IGMP (**I**nternet **G**roup **M**anagement **P**rotocol) ותמיכה בגבולות שידור לרבים (Multicast Boundaries).
- תרגום כתובות רשת עם רכיבי מיעון, ופתרון שמות המקלים על חיבור משרדים קטנים/ביתיים (**S**mall **O**ffice/**H**ome **O**ffice - SOHO) לרשת ולאינטרנט.
- ניתוב AppleTalk משולב.
- תמיכה ב- L2TP (**L**ayer **2** **T**unneling **P**rotocol) על IPSec (**IP Sec**urity), לחיבורי VPN.
- כלי ניהול משופרים. תוסף תוכנה (Add-In) המשמש ככלי ניהול בעל ממשק משתמש גרפי בשם Routing And Remote Access, וכלי שורת הפקודה בשם netsh (Net Shell).
- IAS משופר.

RRAS הוא שירות המשולב באופן מושלם במערכת ההפעלה Windows 2000 Server. הוא פועל עם קשת רחבה של פלטפורמות חומרה ומאות כרטיסי רשת; התוצאה היא פתרון בעלות נמוכה בהרבה מזו של נתבים בינוניים או מוצרי שרת לגישה למרחוק.

RRAS ניתן להרחבה באמצעות ממשקי תכנות יישומים (API - **A**pplication **P**rogramming **I**nterface) בהם יכולים מפתחים להשתמש ליצירת פתרונות רישות מותאמים אישית, וספקים יכולים להשתמש בהם כדי להשתתף בתעשיה הגדלה והולכת של רישות פתוח (Open Internetworking).

מאפייני RRAS המשולבים של Windows 2000, מאפשרים למחשב Windows 2000 Server לתפקד כנתב מרובה פרוטוקולים, נתב חיוג על-פי דרישה ושרת גישה מרחוק.

Multiprotocol Router

מחשב המפעיל את RRAS יכול לנתב IP, IPX ו-AppleTalk בו-זמנית. את כל הפרוטוקולים ברי הניתוב (Routable Protocols) ופרוטוקולי הניתוב (Routing Protocols) מנוהלים באמצעות אותו כלי ניהול.

Demand-Dial Router

מחשב המפעיל את RRAS יכול לנתב IP ו-IPX על קישורי WAN קבועים או על-פי דרישה, כגון קווי טלפון אנלוגיים רגילים או קווי ISDN (**I**ntegrated **S**ervices **D**igital **N**etwork), או על חיבורי VPN תוך שימוש ב-PPTP או L2TP על IPSec.

Remote Access Server

מחשב המפעיל את RRAS יכול לשמש כשרת גישה מרחוק, המספק אפשרות התחברות מרחוק בחיוג או באמצעות VPN ללקוחות המשתמשים ב-IP, IPX, AppleTalk או NetBEUI. השילוב של ניתוב ושירותי גישה מרחוק באותו מחשב יוצר נתב Windows 2000 לגישה מרחוק.

שילוב ניתוב וגישה מרחוק

לפני ש-RRAS יושם ב-Windows NT, פעלו שירותי הניתוב והגישה מרחוק בנפרד. אבל, שני השירותים היו משולבים בזכות פרוטוקול PPP (**P**oint-to-**P**oint **P**rotocol), שהוא חבילת פרוטוקולים, המשמשת בדרך כלל לניהול התקשרות נקודה-לנקודה עבור לקוחות גישה מרחוק. PPP מספק קישור פרמטר משא ומתן (Link Negotiation), תהליך החלפת האישורים (Authentication) עבור לקוחות גישה מרחוק ומשא ומתן של הפרוטוקול ברמת שכבת הרשת (Network Layer Protocol Negotiation). לדוגמה, כאשר אתה מחייג לספק שירותי האינטרנט (ISP) באמצעות PPP, אתה מסכים לגודל המנות שאתה שולח וכיצד הן ימוסגרו (Link Negotiation), אתה נכנס לרשת באמצעות שם משתמש וסיסמה (Authentication) ומקבל כתובת IP (Network Layer Negotiation).

חיבורי ניתוב חיוג על-פי דרישה (Demand-Dial Routing) משתמשים גם הם ב-PPP, לספק את אותם השירותים כמו בחיבורי גישה מרחוק (Link Negotiation, Authentication ו- Network Layer Negotiation). בשל כך, השילוב של ניתוב (הכולל ניתוב חיוג על-פי דרישה) וגישה מרחוק, מתבצעים להגברת תשתית PPP של שרת/לקוח, הזמין לרכיבי הגישה מרחוק.

תשתית PPP של שרת Windows 2000 כוללת תמיכה בסוגי הגישה הבאים:

- ❖ גישה מרחוק בחיוג (Dial-up Remote Access), באמצעות ציוד חיוג כגון קווי טלפון אנלוגיים או קווי ISDN, בין אם כלקוח ובין אם כשרת.
- ❖ גישה מרחוק ל-VPN , בין אם כלקוח ובין אם כשרת.
- ❖ ניתוב חיוג על-פי דרישה בחיוג על-פי דרישה או בחיוג קבוע (בקווי חיוג רגילים או קווי ISDN), בין אם כנתב המתקשר ובין אם כנתב המשיב.
- ❖ ניתוב חיוג על-פי דרישה באמצעות חיוג על-פי דרישה או חיוג קבוע ל-VPN, בין אם כנתב המתקשר ובין אם כנתב המשיב.

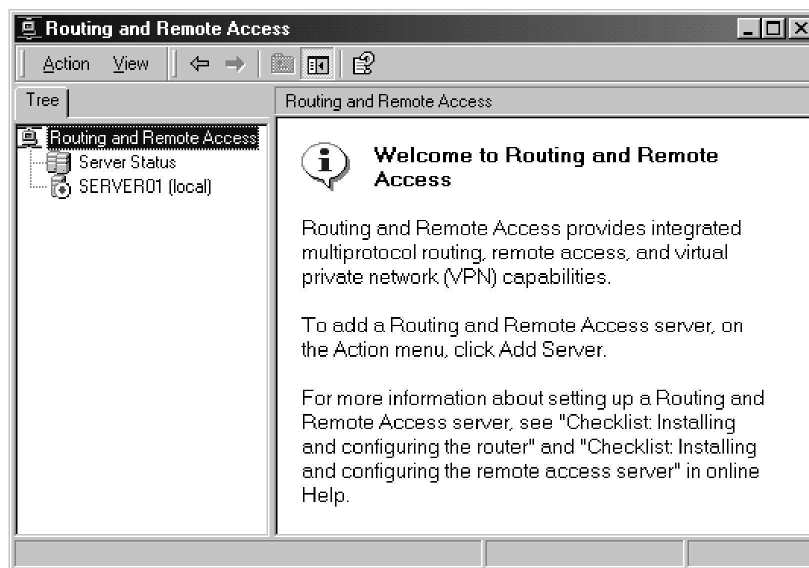
תמיכת LAN ו- WAN

RRAS יכול לפעול בכל כרטיס רשת LAN או WAN הנתמך על ידי שרת Windows 2000, כולל כרטיסים מתוצרת Eicon, Cisco, SysKonnect, Allied ו- USRobotics. למידע נוסף אודות כרטיסי רשת הנתמכים על ידי Windows 2000, פנה לרשימת התאימות לחומרה באתר http://www.microsoft.com/hcl.

התקנה והגדרה

שלא כמו RRAS בגירסה 4.0 של Windows NT, ורוב שירותי הרשת של Windows 2000, אינך בוחר להתקין או להסיר את RRAS באמצעות היישומון Add/Remove Programs שבלוח הבקרה. RRAS של Windows 2000 מותקן כברירת מחדל במצב לא פעיל (Disabled).

תוכל להיעזר בתוסף התוכנה Routing And Remote Access, כדי להפעיל ולהגדיר את RRAS. כברירת מחדל, שרת Windows 2000 מקומי מוגדר כשרת RRAS, כפי שמוצג בתרשים 10.1.



תרשים 10.1 תוסף התוכנה Routing And Remote Access מציג את השרת המקומי, SERVER01, כשרת RRAS לא זמין.

אתה יכול להוסיף מחשבים נוספים על ידי בחירת Routing And Remote Access בחלון Tree, או בצומת Server Status (תרשים 10.1), ואז לפתוח את תפריט Action ולבחור Add Server. לאחר שהוספת שרת בחלון Tree, בחר בשרת אותו אתה מעוניין להפוך לפעיל, פתח את תפריט Action ובחר Configure And Enable Routing And Remote Access (הגדר ואפשר ניתוב וגישה מרחוק). עקוב אחר ההוראות המופיעות באשף Routing And Remote Access Server Setup.

לאחר שהאשף סיים את פעולתו, ניתוב הגישה מרחוק זמין ומוגדר בהתאם לקביעות שביצעת בעת פעולת האשף. כדי לבצע הגדרות נוספות, היעזר בתוסף התוכנה Routing And Remote Access, או בתוכנית השירות של שורת הפקודה netsh.

הערה אם תקליד **?** אחרי הפקודה netsh בשורת הפקודה, **ייתכן שתוכן העזרה יגלוש אל** מעבר לגודל החלון. אם כך יקרה, דע כי ניתן לגלול את חלון שורת הפקודה, להגדילו לגודלו המירבי, או לעבור לצפות בו במסך מלא.

שים לב שכל מחשב ברשת האינטראנט המקבל שירות משרת RRAS, משתמש בכתובת IP פרטית באחד מתחומי הכתובות הבאים:

Network Address Blocks	Address Class
10.0.0.0 - 10.255.255.255	A
172.16.0.0 - 172.31.255.255	B
192.168.0.0 - 192.168.255.255	C

IANA (**I**nternet **A**ssigned **N**umbers **A**uthority), רשות האינטרנט להקצאת מספרים) שמרה במיוחד את הכתובות הללו לשימוש ברשתות פרטיות. ראה מסמך RFC 1918 למידע נוסף בנדון.

תרגיל 1: אפשור RRAS ובחינת תצורה בסיסית

RRAS נמצא כעת במצב לא פעיל (Disabled) ב-Server01. בתרגיל זה תאפשר את פעולת RRAS ואחר כך תבחן את הגדרות ברירת המחדל שלו. בתרגיל אותו תבצע בשלב מאוחר יותר אתה תגדיר את RRAS מחדש, כך שיעמוד בדרישות מורכבות יותר של ניתוב וגישה מרחוק. השלם תרגיל זה ב-Server01.

הליך 1: אפשור RRAS

השלמת הליך זה תגרום לשירות RRAS להיות פעיל ב-Server01. לפני תחילת ההליך, ודא כי ב-Server01 מותקן מודם, וכי הוא מזוהה כהלכה על ידי מערכת ההפעלה. תוכל לעשות זאת באמצעות היישומון Add/Remove Software שבלוח הבקרה.

1. היכנס למחשב Server01 בשם משתמש Administrator ועם הסיסמה password.
2. לחץ Start, הצבע על Programs, הצבע על Administrative Tools ובחר Routing And Remote Access. תוסף התוכנה Routing And Remote Access יופיע, ו- Server01(local) יהיה מסומן בו.
3. הגדל את חלון תוסף התוכנה Routing And Remote Access לגודלו המירבי וקרא את ההודעה המופיעה בחלונית הפרטים.

4. פתח את תפריט Action ולחץ על Configure And Enable Routing And Remote Access (הגדר ואפשר ניתוב וגישה מרחוק). יופיע חלון האשף Routing And Remote Access Server Setup.

5. לחץ Next. המסך Common Configurations יופיע. שים לב שקיימים חמישה נתיבים, בהם תוכל לנוע כדי להגדיר את שרת RRAS. בצעד הבא תבחן את האפשרויות השונות לפני שתגדיר את שרת RRAS לפעול כשרת RAS.

6. ודא שלחצן האפשרויות Internet Connection Server נבחר ולחץ Next.

מסך Internet Connection Server Setup יופיע. שים לב ששרת RRAS מוגדר באחד משני אופנים, כדי לספק לכל המחשבים ברשת את הגישה לאינטרנט. השיטה הראשונה, ICS (**I**nternet **C**onnection **S**haring), מורה לך להשתמש בתיקיה Network and Dial-up Connections, כדי להגדיר אפשרות זו. מאפייני כל קישור בחיוג (Dial-up Connection) כוללים כרטיסיה Sharing באמצעותה ניתן להגדיר אפשרות זו. השיטה השנייה, NAT (**N**etwork **A**ddress **T**ranslation), מוגדרת באמצעות אשף זה. NAT מאפשרת לך להגדיר את השרת, כך שישלח ויקבל מנות מהאינטרנט, בשמם של לקוחות אחרים באינטראנט. רק החומרה בשרת RRAS, המתחבר לאינטרנט, דורשת כתובת IP החוקית למרחבי האינטרנט.

7. לחץ Back. כעת יופיע המסך Common Configurations. קרא, אך אל תשלים את הליכי הניווט המופיעים בסעיף זה. לחץ על לחצן האפשרויות Remote Access Server כדי להגדיר את שרת RRAS לגישת RAS בחיוג (RAS Dial-in access). לחץ על לחצן האפשרויות Virtual Private Network (VPN) server, כדי להגדיר את השרת לגישת VPN (PPTP ו-L2TP). VPN מאפשרת ללקוחות גישה מרחוק להתחבר לרשתות ציבוריות, כגון האינטרנט, ואז ליצור חיבור גישה מרחוק מאובטח לשרת RRAS. לחץ על לחצן האפשרויות Network Router כדי להגדיר את שרת RRAS כך שהמנות ישוגרו בין הרשתות. לחץ על לחצן האפשרויות Manualy Configured Server (הגדרה ידנית של השרת), כדי להשתמש בתוסף התוכנה Routing And Remote Access להגדרת שרת RRAS.

הערה ניתן להגדיר שרת RRAS לשילוב אפשרויות המופיעות במסך Common Configurations. מטרתו של מסך זה היא לסייע לך בהפעלה ראשונית של RRAS. הגדרות נוספות בשלב מאוחר יותר ניתן לבצע באמצעות תוסף התוכנה Routing And Remote Access או באמצעות תוכנית השירות Net Shell.

---

8. לחץ על לחצן האפשרויות Manualy Configured Server ולחץ Next. כעת יופיע המסך Completing The Router And Remote Access Server Setup Wizard.

9. לחץ Finish. תופיע תיבת הודעה שכותרתה Router And Remote Access ובה מצוין כי Routing And Remote Access Service הותקן. אתה נשאל האם יש להפעיל את השירות.

10. לחץ Yes. כעת מופיעות תיבות הודעה שכותרתן Starting Routing And Remote Access ו- Completing Initialization.

הליך 2: בחינת הגדרות ברירת מחדל של RRAS

בהליך זה תבחן את הגדרות ברירת המחדל של שירותי הגישה מרחוק והניתוב. הליך זה מושלם באמצעות תוסף התוכנה Routing And Remote Access. מטרתו של הליך זה היא להציג בפניך את התכונות המופיעות בתוסף התוכנה Routing And Remote Access לפני שתלמד פרטים נוספים אודותיהן, בשיעורים שבהמשך פרק זה.

אזהרה אל תשנה אף אחת מההגדרות בעת בחינת הגדרות ברירת המחדל.

---

1. בחלון Tree, הרחב את Server01 (local). שים לב לחץ הירוק המורה כלפי מעלה שמשמאל לסמל השרת. חץ זה מציין כי RRAS מוגדר ופעיל במחשב זה.

2. פתח את תפריט Action. שים לב שהאפשרות Disable Routing And Remote Access זמינה כעת, מכיון ששרת RRAS מוגדר ופעיל.

3. לחץ Properties. תופיע תיבת הדו-שיח Server01 (local) Properties.

שים לב שהגדרות ברירת המחדל המופיעות בכרטיסיה General מראות כי השרת הוגדר כנתב LAN וחיוג על-פי דרישה (LAN and Demand-dial Router), וגם כשרת גישה מרחוק (Remote Access server).

4. בחר בכרטיסיה Security. שים לב שספק האימות (Authentication Provider) וגם ספק ניהול חשבונות משתמשים (Accounting Provider) הם Windows 2000.

5. לחץ על לחצן Authentication Method.

שים לב שהאפשרויות MS-CHAP ו- MS-CHAP version 2 נבחרות. לאיתור תקלות אימותים, תוכל לסמן את תיבת הסימון Allow Remote Systems To Connect Without Authentication (אפשר למערכות מרוחקות להתחבר ללא אימות). שיטות אימות נוספות נבחרות בהתאם לצרכי לקוח הגישה בחיוג ודרישות אבטחת המידע שלך.

6. לחץ Cancel ובחר בכרטיסיה IP. שים לב שתיבת הסימון Enable IP Routing ותיבת הסימון Allow IP-Based Remote Access And Demand-Dial Connections מסומנות שתיהן. ניתוב IP מאפשר ללקוח חיוג לגשת לכל הרשת. אם אתה מעוניין להגביל את גישת לקוחות החיוג למשאבים בשרת RRAS בלבד, בטל את הסימון בתיבה זו.

האפשרות Allow IP-Based Remote Access And Demand-Dial Connections מאפשרת ל-RRAS לשלוח IPCP, כדי לשאת ולתת לגבי השימוש ב-IP על ממשק הגישה מרחוק או החיוג על-פי דרישה. שים לב שהכרטיסיה IP משמשת גם להגדרת קבלת כתובת IP משרת DHCP, או קבוצת כתובות קבועה המוגדרת בשרת RRAS.

7. בחר בכרטיסיה PPP. בכרטיסיה זו אתה מבצע הגדרות כוללות לתמיכת PPP עבור לקוחות הגישה מרחוק. אפשרויות אלו ידונו בהרחבה בשיעור 3, "RAS".

8. בחר בכרטיסיה Event Logging (יומן אירועים). מכאן אתה מגדיר את כמות הנתונים שאתה מעוניין לאסוף אודות אירועי RRAS המתרחשים בשרת. לאיתור תקלות, לחץ על לחצן האפשרויות Log The Maximum Amount Of Information וסמן את תיבת הסימון Enable Point-To-Point Protocol (PPP) Logging. כדי למטב (Optimize) את ביצועי השרת, סמן את לחצן האפשרויות Disable Even Logging.

9. לחץ Cancel.

10. בחלון Tree, לחץ על Routing Interfaces.

רשימת ממשקי הניתוב תופיע בחלונית הפרטים. הממשק Loopback הוא מחסנית הפרוטוקול המקומית בשרת RRAS. Local Area Connections הוא ממשק כרטיס הרשת בשרת RRAS, המחובר לרשת שלך. Internal היא פעילות הניתוב ב-RRAS. אם הניתוב אינו מאופשר (Disabled) יופיע הערך Non-operational בעמודה Operational Status של ממשק Internal.

11. בחלון Tree, לחץ על Ports. שים לב שהמודם, או התקן WAN שלך מופיע בחלונית הפרטים. שים לב גם לכך, שהגדרות ברירת המחדל של VPN הן חמש מיני-יציאות PPTP (Miniport) וחמש מיני-יציאות L2TP. האפשרות Parallel Device(s) המופיעה בחלונית הפרטים זמינה, לשם תמיכה בחיבור כבל ישיר (Direct Cable Connection) בין שני מחשבים. אם מותקנת במחשב יציאה מקבילית יחידה המוגדרת כ-LPT1, אזי שם החיבור יהיה Direct Parallel (LPT1). אם לקוח מרוחק מתחבר ליציאה, אך הביצועים ירודים, או שאתה מנסה לאתר תקלות בחיבור, בחר ביציאה (Port) אליה מחובר הלקוח, פתח את תפריט Action ובו בחר Status. פעולה זו תציג בפניך רישומי רשת (Network Registration), סטטיסטיקה (Statistics) ונתוני שגיאות (Error Information) לגבי חיבור זה.

12. ודא כי בחלון Tree נבחר Ports, פתח את תפריט Action ובחר Properties.

תיבת הדו-שיח Ports Properties תופיע, וממנה תגדיר את מספר היציאות המאושרות לכל סוג יציאה (הדבר נכון לגבי חיבורי VPN בלבד), ותקבע אם חיבורים ליציאה זו הם חיבורים פנימה בלבד, או שהם דו-כיווניים (פנימה והחוצה). אתה גם מגדיר את מספר הטלפון של התקן זה. מאפיין זה משמש במצב בו זיהוי מיקום המתקשר (Call-Station-ID) מוגדר כמדיניות הגישה מרחוק, חומרת החיוג ותוכנת מנהל התקן החיוג אינם תומכים בשיחה מזוהה (Caller ID), או אם אתה מאפשר ריבוי קישורים (Multilink) עם פרוטוקול Bandwidth) BAP Allocation Protocol). אם אתה מגדיר יציאת VPN, הקלד את כתובת ה-IP של היציאה, ולא את מספר הטלפון.

13. לחץ Cancel.

14. בחלון Tree, לחץ על Remote Access Clients. אם לקוח גישה מרחוק מחובר לשרת RRAS, תציג חלונית הפרטים את הלקוח המחובר, את משך השיחה ואת מספר היציאות המוקצות לשיחה זו (Multilink).

15. בחלון Tree, הרחב את IP Routing ולחץ על General. שים לב שהמידע המופיע בחלונית הפרטים, נראה דומה לזה המופיע בחלונית הפרטים של Routing Interfaces.

16. פתח את תפריט Action ובחר New Routing Protocol. תופיע תיבת הדו-שיח New Routing Protocol. שים לב ששלושה פרוטוקולים מופיעים כברירת מחדל: NAT, OSPF ו- RIP גירסה 2. בפרוטוקולים אלה נדון בשיעור 2, "מאפייני שירות וניתוב גישה מרחוק".

17. לחץ Cancel.

18. לחץ על Internal בחלונית הפרטים ופתח את תפריט Action.

שים לב שרבות מאפשרויות ניטור הממשק בתפריט Action זמינות. האפשרות Properties משמשת להגדרת הגדרות נתב כלליות בשרת RRAS.

בחן את מאפייני ממשק Internal וממשק Local Area Connections ואז חזור לתוסף התוכנה Routing And Remote Access.

הצומת Static Routes בחלון Tree משמש לצפייה והגדרה של ניתובים נוספים לרשתות שונות. כלי זה הוא המקביל הגרפי של פקודת Route בשורת הפקודה.

הצומת DHCP Relay Agent מאפשר לבקשות ותשובות לבקשות DHCP להישלח מרשת אחת לאחרת. מאפיין זה מאפשר לשרת יחיד, המפעיל את שירות DHCP, לספק נתוני תצורת כתובות IP ללקוחות DHCP (BOOTP מותאם) וללקוחות המאפשרים BOOTP ברשתות אחרות הנגישות דרך נתב זה.

הצומת IGMP מאפשר לך להגדיר את הגדרות Internet Group Messaging Protocol.

19. בחלון Tree, לחץ על Remote Access Logging.

הערה אם אתה משתמש בשרת RADIUS **לאימות ורישומי יומנים**, התיקיה Remote Access Logging **לא תופיע ב-**RRAS.

בחלונית הפרטים מופיע Local File ובעמודת התיאור (Description) מופיע הנתיב לתיקיה LogFiles.

20. לחץ לחיצה כפולה על Local File בחלונית הפרטים. תופיע תיבת הדו-שיח Local File Properties.

הכרטיסיות Settings ו- Local File משמשות להגדרת רישומי היומן (Logging). היעזר בנתונים המופיעים בכרטיסיה Settings, כדי להגדיר את כמות הנתונים שאתה מעוניין לשמר אודות אימות גישה מרחוק, ניהול ומצב.

21. בחר בכרטיסיה Local File. היעזר בנתונים המופיעים בכרטיסיה Local File, כדי להגדיר את מבנה קובץ היומן (Log File), כאשר נוצרים קבצי יומן חדשים וכאשר קבצי יומן מאוחסנים. מומלץ להעביר את תיקיית קבצי היומן למחיצה שאינה מחיצת האתחול (Boot Partition).

22. לחץ Cancel.

23. בחלון Tree, לחץ על Remote Access Policies. הגדרת מדיניות ברירת המחדל לגישה מרחוק, Allow Access If Dial-In Permission Is Enabled, תופיע בחלונית הפרטים.

24. לחץ לחיצה כפולה על Allow Access If Dial-In Permission Is Enabled.

תיבת הדו-שיח Allow Access If Dial-In Permission Is Enabled Properties תופיע.

25. לחץ Edit. תיבת הדו-שיח Time Of Day Constraints תופיע.

שים לב, שההרשאות לחיוג פנימה מאפשרות כניסה בחיוג בכל שעות היממה.

26. לחץ Cancel. שים לב שלחצן האפשרויות Deny Remote Access Permission נבחר. דבר זה מצביע על כך, שלקוחות המסתמכים על גישה מבוססת פרופיל, לא יוכלו לבצע גישה אף פעם, אלא אם כן פרופיל זה נאכף על ידי הגדרות ייחודיות למשתמש.

27. לחץ Add. תיבת הדו-שיח Select Attribute תופיע. תיבת דו-שיח זו מציגה רשימה של מאפיינים שונים של חיבורים, שיכולים להיות משויכים לפרופיל זה. משתמשים העומדים בתנאים המפורטים בפרופיל יקבלו גישה או שגישתם תידחה.

28. לחץ Cancel.

29. לחץ על Edit Profile, וסקור את הכרטיסיות ואת ההגדרות השונות הזמינות בעת עריכת פרופיל. שים לב שרבות מההגדרות, אותן תוכל לבצע בפרופיל, תוכל לבצע גם בנפרד ממנו, באמצעות תוסף התוכנה Routing And Remote Access.

30. לחץ Cancel.

31. לחץ Cancel פעם נוספת, כדי לסגור את תיבת הדו-שיח Allow Access If Dial-In Permission Is Enabled Properties.

32. מזער את תוסף התוכנה Routing And Remote Access; תשתמש בו בתרגיל הבא.

הליך זה הוביל אותך בנבכי תוסף התוכנה Routing And Remote Access. יתר הפרק בוחן את מאפייני RRAS.

הערה ניתן להגדיר את RRAS גם משורת הפקודה, תוך שימוש בפקודה netsh. אין חובה להשתמש בתוסף התוכנה של Routing And Remote Access.

ביטול RRAS

למרות שממשק Windows 2000 לא נועד להקל עליך בהסרת RRAS, תוכל שלא לאפשר אותו באמצעות תוסף התוכנה Routing And Remote Access. בחלון Tree, בחר במחשב בו אתה מעוניין לבטל את RRAS, פתח את תפריט Action וממנו בחר באפשרות Disable Routing And Remote Access. אי אפשור השירות מסיר את כל הגדרות רישום המערכת (Registry) הנוגעות לניתוב וגישה מרחוק (Routing and Remote Access).

באפשרותך גם לרענן את הגדרות RRAS, אם תבטל קודם כל את השירות ואז תאפשר אותו מחדש.

הערה אם תבטל את RRAS, כל ההגדרות הנוכחיות של השירות, כולל תצורת פרוטוקול ניתוב וממשקי חיוג על-פי דרישה, יוסרו וכל הלקוחות המחוברים ברגע ביטול השירות ינותקו מהמחשב.

Authentication and Authorization

ההבחנה בין אימות (Authentication) ואישור (Authorization) חשובה להבנת אופן הרשאת ניסיונות ההתחברות או דחייתם:

- **אימות** (Authentication) – מוודא את נתוני המשתמש (User Credentials) בזמן ניסיון ההתחברות. תהליך זה כולל שליחת נתוני המשתמש מלקוח הגישה מרחוק לשרת הגישה מרחוק במבנה טקסט נקי (Clear Text) או במבנה מוצפן (Encrypted), הנעזר בפרוטוקול אימות (Authentication Protocol).

- **אישור** (Authorization) – מוודא שניסיון ההתחברות מורשה על בסיס מדיניות. אישור מתבצע לאחר אימות מוצלח.

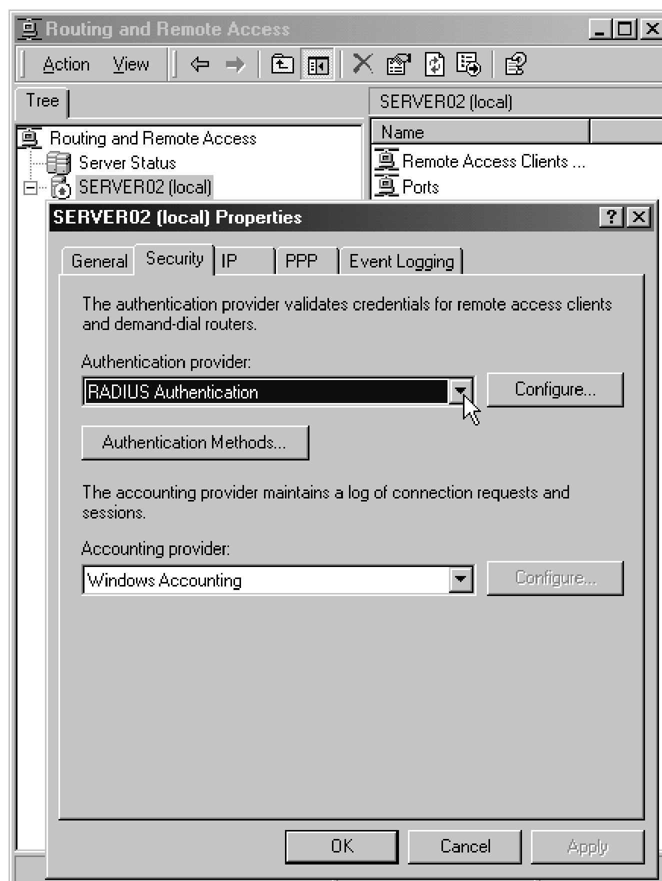
כדי שניסיון התחברות יתאפשר, חייב החיבור להיות מאומת ומאושר. ניסיון ההתחברות יכול להיות מאומת באמצעות נתוני המשתמש המתאימים, אך לא יהיה מאושר. במקרה כזה ייכשל ניסיון ההתחברות.

אם שרת הגישה מרחוק מוגדר עם אימות Windows, מערכת אבטחת המידע של Windows 2000 מוודאת את נתוני אימות המשתמש (User Credentials), את מאפייני החיוג עבור חשבון המשתמש ואת מדיניות הגישה מרחוק, המאוחסנת באופן מקומי, המאשרת את ההתחברות. אם ניסיון ההתחברות מאומת וגם מאושר, תתבצע התחברות מוצלחת.

אם בשרת הגישה מרחוק מוגדר אימות, באמצעות שירות אימות מרחוק של לקוחות חיוג (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice - RADIUS), מועברים נתוני המשתמש הנשלחים מהלקוח לשרת RADIUS, עבור אימות ואישור. אם ניסיון ההתחברות מאומת וגם מאושר, שולח שרת RADIUS הודעת Accept חזרה לשרת הגישה מרחוק והחיבור מתבצע. אם ההתחברות אינה מאומתת או שאינה מאושרת, שולח שרת RADIUS הודעת Reject חזרה לשרת RAS ותהליך ההתחברות נכשל.

אם שרת RADIUS הוא שרת מבוסס Windows 2000, המפעיל שירות אימות אינטרנט (Internet **A**uthentication **S**ervice - IAS), מבצע שרת IAS אימות באמצעות מערכת האבטחה של Windows 2000, ואישור באמצעות מאפייני החיוג של חשבון המשתמש ומדיניות הגישה מרחוק המאוחסנת בשרת IAS.

הגדרת ספק האימות עבור RRAS נעשית בכרטיסיה Security שבתיבת הדו-שיח Properties של נתב גישה מרחוק בתוסף התוכנה Routing And Remote Access (תרשים 10.2), או באמצעות תוכנית השירות netsh.



תרשים 10.2 מאפייני שרת RRAS במחשב Server02, כאשר נבחרה האפשרות ששרת RADIUS יהיה ספק האימות.

סיכום שיעור

RRAS של Windows 2000 ממשיך את ההתפתחות של שירותי ניתוב מרובה פרוטוקולים וגישה מרחוק לפלטפורמות Windows. RRAS משולב במערכת ההפעלה Windows 2000 Server ופועל עם קשת רחבה של פלטפורמות חומרה ומאות רבות של כרטיסי רשת. המאפיינים המשולבים של RRAS של Windows 2000 מאפשרים לשרת Windows 2000 לתפקד כנתב מרובה פרוטוקולים, נתב חיוג על-פי דרישה ושרת גישה מרחוק. RRAS משתמש ב-PPP כדי לשאת ולתת לגבי חיבורי נקודה-לנקודה ללקוחות גישה מרחוק בחיוג. PPP מנהל משא ומתן לגבי פרמטר הקישור (Link Parameter Negotiation), מבצע את חלופת נתוני האימות של המשתמש ומנהל את המשא ומתן בעבור פרוטוקול שכבת הרשת (Network Layer Protocol). תוכל להשתמש בתוסף התוכנה Routing And Remote Access כדי לאפשר ולהגדיר את RRAS, או כדי לבטל את השירות. כדי שניסיון התחברות יסתיים בהצלחה הוא צריך להיות מאומת וגם מאושר.

שיעור 2: מאפייני שירות ניתוב וגישה מרחוק

RRAS של Windows 2000 כולל מיגוון רחב של מאפיינים התומכים בניתוב שידור IP ליחיד ולרבים (IP Unicast ו-IP Multicast), ניתוב IPX, AppleTalk, גישה מרחוק ותמיכה ב-VPN.

לאחר שיעור זה, תוכל

- לתאר את המאפיינים העיקריים של RRAS ב-Windows 2000.

זמן לימוד משוער: 25 דקות

IP Unicast

Windows 2000 מספקת תמיכה נרחבת לניתוב שידור IP ליחיד (ניתוב לכתובת IP של יעד Unicast), תוך שימוש בפרוטוקולי ניתוב שידור IP ליחיד ומאפיינים של נתב Windows 2000. המושג Unicasting מכוון למצב בו שני מחשבים יוצרים ביניהם חיבור דו-כיווני (Two-way Connection) מנקודה-לנקודה, לצורך העברת נתונים ביניהם. במושג ניתוב Unicast - הכוונה היא לנתב או נתבים המעבירים מנות נתונים בין שני חיבורי נקודה-לנקודה (Point-to-Point Connection). יישום ניתוב Unicast יכול להיות פשוט או מורכב, בהתאם לרישות IP שלך, השימוש בשרת DHCP להקצאת נתוני תצורת כתובות IP, קישוריות לאינטרנט, קיומם של שרתים שאינם פועלים עם מערכות ההפעלה של Microsoft או שהם מיושנים וסיבות נוספות.

הטבלה הבאה מתארת את המרכיבים השונים שבניתוב שידור IP ליחיד.

מאפיין	תיאור
ניתוב IP קבוע	עם תכונה מורשת זו של פרוטוקול TCP/IP של Windows 2000, תוכל לנהל נתבים קבועים (סטטיים) באמצעות תוסף התוכנה Routing And Remote Access, או באמצעות netsh. תוכנית השירות routemon אינה נתמכת בסביבת Windows 2000.
RIP גירסה 1 או 2	פרוטוקול ניתוב מרחק-וקטורי (Distance-Vector), בו נעשה בדרך כלל שימוש ברשתות IP קטנות/בינוניות.
OSPF	פרוטוקול ניתוב Link-State, בו נעשה בדרך כלל שימוש ברשתות IP בינוניות/גדולות. פרוטוקול זה יעיל יותר מ- RIP באופן משמעותי, מפני שהוא משתמש באלגוריתמים מורכבים הרבה יותר, כדי למצוא את הנתיב הטוב ביותר בין שתי נקודות.

מאפיין	תיאור
DHCP Relay Agent	סוכן המוסר הודעות DHCP בין לקוחות ושרתי DHCP בסגמנטים שונים של הרשת. דבר זה מאפשר לשרת DHCP לתת שירותים למספר רב של תחומי רשת (Network Scopes). ראה RFC 1542 למידע נוסף.
Network Adapter Translation (NAT)	רכיב המתרגם כתובות רשת ויוצר חיבור מתורגם בין רשתות הממוענות באופן פרטי והאינטרנט. דבר זה מאפשר להשתמש ברשת הפנימית במיעון שאינו חוקי באינטרנט, ועדיין מאפשר גישה לאינטרנט.
IP Packet Filtering	היכולת לאבחן איזו תעבורה מאושרת לעבור אל ומאת כל ממשק, בהתבסס על מסננים המוגדרים על ידי ערכי כתובת IP של המקור ושל היעד, מספרי יציאות TCP ו-UDP, סוגים וקודים של ICMP ומספרי פרוטוקול IP. זהו מאפיין אבטחה חשוב ביותר.
ICMP Router Discovery	היכולת לפרסם מדי תקופה ולהגיב לשידולי נתבים מארחים לתמיכה בנתב ICMP Router Discovery על ידי מארחים בסגמנט רשת.

IP Multicast

Windows 2000 תומכת בשליחה, בקבלה ובהעברה של תנועת שידור IP לרבים (IP Multicast Traffic). תנועת שידור IP לרבים נשלחת למארח בודד, אך מעובדת על ידי מספר מארחים המאזינים לסוג תנועה זה, המיועד למארח בודד. דבר זה משמש בדרך כלל להעברת נתוני זמן-אמת למספר משתמשים, כגון בעת העברת מצגת משודרת ברשת. רכיבי שידור IP לרבים של RRAS מאפשרים לך לשלוח ולקבל תנועת שידור IP לרבים מלקוחות גישה מרחוק, וספקי שירותים המאפשרים זאת באינטרנט, או ברשת האינטראנט הפנימית של הארגון.

הטבלה שלהלן מתארת את הרכיבים השונים של ניתוב שידור IP לרבים.

מאפיין	תיאור
העברת שידור לרבים (Multicast)	באמצעות מאפיין אינטרנטי זה של פרוטוקול TCP/IP עבור Windows 2000, אתה יכול לצפות בטבלת העברת שידור IP לרבים, תוך שימוש בתוסף התוכנה Routing And Remote Access, או שתוכל להיעזר בתוכנית השירות של שורת הפקודה - netsh.
IGMP גירסה 1 ו-2	פרוטוקול TCP/IP למעקב אחר חברויות בקבוצות שידור לרבים בסגמנטים צמודים ברשת.

מאפיין	תיאור
העברה וניתוב ייחודיים	כשאתה משתמש בפרוטוקול הניתוב IGMP, ומגדיר ממשקים עבור מצב IGMP Router ועבור מצב IGMP Proxy, נתב Windows 2000 יכול לתמוך בהעברת שידור לרבים ובניתוב לתצורות ייחודיות.
גבולות שידור לרבים (Multicast Boundaries)	גבולות שידור לרבים (גבולות להעברת תנועות שידור IP לרבים) יכולים להתבסס על כתובת קבוצת שידור IP ברבים, משך TTL (אורך חיים) בכותרת IP, או על הכמות המירבית של תנועת שידור ברבים, בקילו-בתים לשנייה.

IPX Support

נתב שרת Windows 2000 הוא נתב מלא ל-IPX התומך ב- RIP עבור IPX (פרוטוקול הניתוב העיקרי המשמש לרישות IPX ברשתות רחבות היקף, Internetworks), SAP עבור IPX של Novell NetWare (פרוטוקול לאיסוף והפצה של שמות שירותים וכתובות), והעברת שידור NetBIOS על IPX.

הטבלה הבאה מתארת את הרכיבים השונים של ניתוב IPX.

מאפיין	תיאור
סינון מנות IPX	האפשרות לקבוע איזו תנועה מורשית אל ומאת כל ממשק, בהתבסס על מסננים הנקבעים על-פי הערכים של מקור ויעד רשת IPX, צומת, מספרי שקע (Socket) וסוג מנה.
RIP עבור IPX	פרוטוקול ניתוב מבוסס מרחק-וקטור, המשמש ברשתות IPX רחבות היקף. RRAS גם מאפשר לך להגדיר נתיבי IPX קבועים ומסנני נתיב RIP.
SAP עבור IPX	SAP הוא פרוטוקול פרסום מבוסס מרחק-וקטור, המשמש בדרך כלל ברשתות IPX רחבות היקף לפרסום שירותים ומיקומם. RRAS גם מספק את היכולת להגדיר שירותי SAP קבועים ומסננים לשירות SAP. מסנני שירות SAP מפחיתים תנועת SAP לא דרושה, כך שלא תישלח בחיבורי RRAS.
NetBIOS over IPX	NetBIOS על IPX משמש את רכיבי הרישות של Microsoft לתמיכה ברכיבי שיתוף קבצים ומדפסות. RRAS יכול גם להעביר שידורי NetBIOS על IPX ולהגדיר שמות NetBIOS קבועים.

AppleTalk

RRAS של Windows 2000 יכול לשמש גם כנתב AppleTalk, על ידי העברת מנות AppleTalk ותמיכה בשימוש בפרוטוקול תחזוקת טבלת ניתוב (**R**outing **T**able - RTMP **M**aintenance **P**rotocol). Windows 2000 תומכת במחסנית פרוטוקול AppleTalk ובתוכנות ניתוב AppleTalk, כך ששרת מבוסס Windows 2000 יכול לתקשר עם רשת Macintosh, מבוססת AppleTalk ולספק לה שירותים.

רוב רשתות AppleTalk הגדולות, כמו כל רשת גדולה אחרת, אינן רשת פיסית גדולה אחת, בה כל המחשבים מחוברים לאותה מערכת כבלים ברשת. במקום זאת, אלו הן רשתות אינטרנט של AppleTalk, שהן רשתות פיסיות קטנות יותר, המחוברות ביניהן באמצעות נתבים.

שרת מבוסס Windows 2000 יכול לספק ניתוב ותמיכה ב-Seed Routing (במקור ניתוב). RRAS אינו מגביל את מספר כרטיסי הרשת במחשב, שיכולים לתמוך ברשת AppleTalk, הבנויה ממספר רשתות פיסיות קטנות אשר מקושרות באמצעות נתבים.

Demand-Dial Routing

Windows 2000 תומכת בניתוב חיוג-על-פי-דרישה (Demand-Dial Routing), ניתוב מנות בקישורי נקודה-לנקודה, כגון קווי טלפון רגילים או ISDN. ניתוב חיוג-על-פי-דרישה מאפשר לך להתחבר לאינטרנט, לקשר בין סניפים של הארגון או ליישם קישורי VPN של נתב-לנתב.

תנועת IP ו-IPX יכולה להיות מועברת בממשקי חיוג-על-פי-דרישה באמצעות קישורי WAN קבועים או על-פי דרישה. לחיבורים על-פי-דרישה (On-Demand Connections) יוצר RRAS באופן אוטומטי חיבור PPP לנקודת הקצה המוגדרת, כאשר מתקבלת תנועה התואמת לניתוב קבוע.

Remote Access

RRAS מאפשר למחשב להיות שרת גישה מרחוק, זאת אומרת, לקבל חיבורי גישה מרחוק בחיוג מלקוחות גישה מרחוק המשתמשים בטכנולוגיות חיוג רגילות, כגון קווי טלפון רגילים וקווי ISDN. נושא הגישה מרחוק נידון בהרחבה בשיעור 3, "RAS".

VPN Server

RRAS מאפשר למחשב להיות שרת VPN, תוך כך שהוא תומך ב-PPTP וב-L2TP על IPSec, ומקבל חיבורי גישה מרחוק ל-VPN וגם חיבורי נתב-לנתב (חיוג-על-פי-דרישה, Demand-Dial) ל-VPN, מלקוחות גישה מרחוק ונתבים מתקשרים. VPN נידון בהרחבה בשיעור 4, "VPN".

RADIUS Client-Server

שירות אימות אינטרנט (**I**nternet **A**uthentication **S**ervice - IAS) של Windows 2000 הוא יישום Microsoft של שרת RADIUS. IAS מרכז את האימות (**A**uthentication), האישור (**A**uthorization), הבקרה (**A**uditing) וניהול החשבונות (**A**ccounting) - או בקיצור ה - **AAAA**, של חיבורים מרחוק ל-VPN ולחיבורי חיוג-על-פי-דרישה, והוא יכול לשמש בשיתוף עם RRAS של Windows 2000. IAS מאפשר את השימוש ברשת של יצרן אחד או יותר של ציוד גישה מרחוק או VPN.

ספקי שירותי אינטרנט (**I**nternet **S**ervice **P**rovider - ISP) וארגונים גדולים, המתחזקים שירות גישה מרחוק עבור עובדיהם, ניצבים בפני האתגר הגדל והולך של ניהול נושא הגישה מרחוק מנקודת ניהול אחת - ללא קשר לסוג הציוד המשמש לגישה מרחוק. תקן RADIUS תומך באפשרות זו בסביבות אחידות או מגוונות. RADIUS הוא פרוטוקול שרת-לקוח, דבר המאפשר לציוד הגישה מרחוק של לקוחות RADIUS להעביר בקשות אימות וניהול חשבונות לשרת RADIUS.

לשרת RADIUS יש גישה לנתוני חשבון המשתמש, והוא יכול לבחון ולבצע אימותי גישה מרחוק. אם הנתונים שנמסרו על ידי המשתמש מאומתים, וניסיון החיבור של הלקוח מאושר – מאשר שרת RADIUS את גישת המשתמש, בהתבסס על תנאים מסוימים, ורושם את חיבורי הגישה מרחוק כאירועי ניהול חשבונות (Accounting Events).

RADIUS תומך באימות ואישור משתמש בגישה מרחוק, ומאפשר לנתוני ניהול החשבונות להיות מנוהלים במיקום מרכזי אחד במקום לנהל אותם על כל שרת גישה לרשת (**N**etwork **A**ccess **S**erver- NAS) בנפרד. משתמשים מתחברים למחשב NAS-תואם-RADIUS, כגון מחשב מבוסס Windows 2000 המפעיל RRAS, המשמש כלקוח RADIUS ומעביר את בקשות האימות לשרת IAS מרכזי אחד.

הערה שרת Windows 2000 **יכול לשמש הן** כשרת RADIUS **והן כלקוח** RADIUS בעת **ובעונה** אחת.

SNMP MIB

Windows 2000 ו-RRAS מתפקדים גם כסוכן של פרוטוקול ניהול לרשת פשוטה (SNMP-Simple Network Management Protocol), התומך ב- Internet MIB II (כפי שמתואר במסמך RFC 1213). תחנת ניהול רשת (Network Management Station - NMS), כגון HP Open View, יכולה להדר (Compile) את MIB לנהל אירועי שכבת רשת IP, המשויכים לפעילויות נתב גישה מרחוק של Windows 2000. המחשב המפעיל את RRAS חייב גם להפעיל את שירות SNMP, הנקרא גם סוכן SNMP (SNMP Agent), כדי שניתן יהיה לנהל אותו באמצעות NMS. מעבר ל- Internet MIB II, תמיכת RRAS בהרחבות MIB נוספות, שיכולות להיות מהודרות על ידי NMS לתמיכה ב-RRAS, עשויות לכלול:

- MIB טבלת העברת IP (IP Forwarding Table MIB)
- גירסה 2 של Microsoft RIP עבור פרוטוקול Internet MIB
- Wellfleet-Series-7-MIB עבור OSPF
- Microsoft BOOTP עבור Internet Protocol MIB
- IPX MIB של Microsoft
- RIP ו-SAP של Microsoft עבור IPX MIB
- Internet Group Management Protocol MIB
- IP Multicast Routing MIB

הערה קיימת גם תמיכת MIB בפונקציונליות מערכת ההפעלה Windows 2000 Server, בפונקציונליות LAN Manager MIB מיושן, ובשירותים WINS, DHCP ו-IIS. IPX נתמך גם על ידי שירות SNMP, אולם כדי לאפשר זאת חייב להיות מותקן פרוטוקול TCP/IP.

תמיכת API לרכיבי צד-שלישי

ל-RRAS יש קבוצות API (Application Programming Interface, ממשק תכנות יישומים), שפורסמו במלואן עבור פרוטוקול ניתוב שידור IP ליחיד ולרבים (Unicast ו-Multicast) ולתמיכה בתוכנית שירות לניהול. מפתחי פרוטוקול ניתוב יכולים לכתוב פרוטוקולים וממשקים נוספים, ישירות לתוך ארכיטקטורת RRAS. יצרני תוכנה אחרים יכולים גם להיעזר בממשקי תכנות היישומים לניהול RRAS (RRAS Administration APIs) כדי ליצור את כלי הניהול המותאמים שלהם.

סיכום שיעור

RRAS של Windows 2000 כולל קשת רחבה של מאפיינים ותכונות. Windows 2000 תומכת בניתוב שידור IP ליחיד (ניתוב שידור כתובת יעד IP ליחיד); היא גם תומכת בשליחה, קבלה והעברה של תנועת שידור IP לרבים, ויכולה לשמש כנתב IPX לכל דבר. בנוסף, RRAS תומך גם ב-AppleTalk, ניתוב חיוג-על-פי-דרישה, גישה מרחוק ו-VPN. מחשב Windows 2000 Server יכול גם לשמש כשרת RADIUS ולפעול כסוכן SNMP. לבסוף, ל-RRAS יש קבוצות API שפורסמו במלואן עבור פרוטוקול ניתוב שידור IP ליחיד ולרבים (Unicast ו-Multicast) ולתמיכה בתוכנית שירות לניהול.

שיעור 3: RAS

טכנולוגיית הגישה מרחוק (Remote Access) של Windows 2000 מאפשרת ללקוחות מרוחקים להתחבר לרשת הארגונית או לאינטרנט. שיעור זה יתאר באופן כללי את נושא הגישה מרחוק, וידון בנושא חיבורי גישה מרחוק בחיוג, אבטחת גישה מרחוק וניהול גישה מרחוק. השיעור מתמקד בחלק של שירות הגישה מרחוק של RRAS. מכאן ואילך ישמש הקיצור RAS להתייחסות לשירות הגישה מרחוק (Remote Access Service) של RRAS.

בסיומו של שיעור זה, תוכל

- לתאר כיצד פועלת הגישה מרחוק, כולל חיבורי גישה מרחוק בחיוג ואבטחת גישה מרחוק.
- לנהל גישה מרחוק, כולל ניהול משתמשים, כתובות, גישות ואימות.

זמן לימוד משוער: 35 דקות

מבוא לגישה מרחוק

ב-RAS של Windows 2000, לקוחות גישה מרחוק מחוברים למשאבים המצויים בשרת הגישה מרחוק (חיבוריות גישה מרחוק מנקודה-לנקודה), או שהם מחוברים למשאבים שבשרת RAS ולמשאבים ברשת, אליהם יש לשרת הגישה מרחוק גישה (חיבוריות גישה מרחוק מנקודה-ל-LAN). סוג החיבוריות האחרון שהוזכר, מאפשר ללקוחות הגישה מרחוק גישה למשאבים, כאילו היו מחוברים באופן פיסי ישירות לרשת.

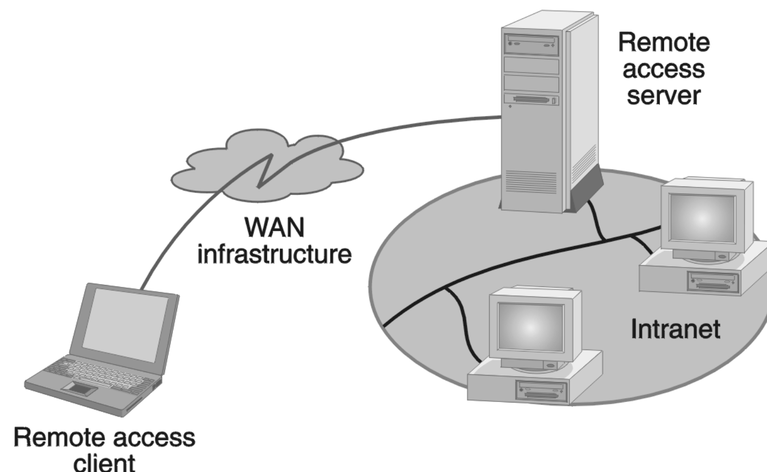
שרת גישה מרחוק של Windows 2000 מאפשר שתי שיטות חיבור:

- **גישה מרחוק בחיוג** – בגישה מרחוק בחיוג (Dial-up Remote Access) משתמש לקוח הגישה מרחוק בתשתית הטלפוניה, כדי ליצור חיבור פיסי או וירטואלי זמני, ליציאה בשרת הגישה מרחוק. לאחר שנוצר החיבור הפיסי או הוירטואלי, נידונים יתר פרטי ההתחברות.
- **גישה מרחוק VPN** – בגישה מרחוק באמצעות רשת פרטית וירטואלית, משתמש לקוח VPN ברשת IP רחבת היקף, כדי ליצור חיבור נקודה-לנקודה עם שרת RAS המשמש כשרת VPN. לאחר שנוצר חיבור וירטואלי מנקודה-לנקודה, נידונים יתר פרטי ההתחברות.

הערה שיעור זה מתמקד בעיקר בנושא גישה מרחוק בחיוג (Dial-up Remote Access), אולם, נושאים רבים בו עשויים להיות תואמים גם לגישה מרחוק VPN. להבנה מלאה של VPN, קרא את שיעור זה וסקור את שיעור 4, "VPN".

Dial-up Remote Access Connections

חיבורי גישה מרחוק בחיוג (Dial-up Remote Access Connections) כוללים את לקוח הגישה מרחוק, שרת הגישה מרחוק ואת תשתית הרשת המרחבית (WAN), כפי שמוצג בתרשים 10.3.



תרשים 10.3 מרכיבי חיבור גישה מרחוק בחיוג.

Remote Access Client

Windows 2000, Windows NT גירסה 3.51 ומעלה, Windows 95, Windows 98, Windows for Workgroups, MS-DOS ולקוחות גישה מרחוק של Microsoft LAN Manager יכולים כולם להתחבר לשרת גישה מרחוק של Windows 2000. כמעט כל לקוחות הגישה מרחוק המפעילים את פרוטוקול PPP, כולל לקוחות UNIX ומקינטוש, יכולים להתחבר לשרת גישה מרחוק של Windows 2000.

לקוח גישה מרחוק של Microsoft מסוגל גם לחייג לשרת SLIP (**S**erial **L**ine **I**nterface **P**rotocol). SLIP הוא פרוטוקול חיוג מיושן (Legacy) שאינו מספק את האבטחה, הביצועים או האמינות של PPP. שרת RAS של Windows 2000 אינו תומך בחיבורי SLIP בחיוג פנימה (Dial-in).

Remote Access Service Server

שרת הגישה מרחוק של Windows 2000 מקבל חיבורים בחיוג ומעבירי מנות בין לקוחות גישה מרחוק והרשת אליה הוא (השרת) מחובר.

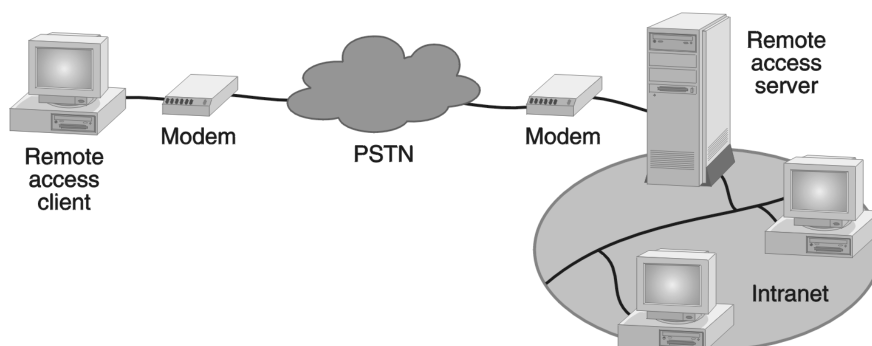
ציוד חיוג ותשתית WAN

החיבור הפיסי או הלוגי בין שרת הגישה מרחוק ולקוח הגישה מרחוק, מתאפשר הודות לציוד חיוג המותקן בלקוח ובשרת, ולתשתית הטלפוניה. טיבם של ציוד החיוג ושל תשתית הטלפוניה משתנה, בהתאם לסוג החיבור המתבצע.

Public Switched Telephone Network - PSTN

PSTN (רשת מיתוג טלפון ציבורית), הידועה גם בשם שירות טלפון ישן פשוט (POTS - **P**lain **O**ld **T**elephone **S**ervice), היא מערכת הטלפונים האנלוגית שנועדה לשאת את התדרים המינימליים להעברת קולות אנושיים. מכיון ש-PSTN לא נועדה להעברת נתונים, קיימת מגבלה לגבי כמות הסיביות המירבית בה יכול לתמוך חיבור PSTN. ציוד החיוג כולל מודם אנלוגי ללקוח הגישה מרחוק ועבור שרת הגישה מרחוק. בארגונים גדולים שרת הגישה מרחוק מחובר לבנק מודמים, העשוי להכיל עד כמה מאות כרטיסי מודם. עם מודם אנלוגי בשני הקצוות (שרת ולקוח), קצב הסיביות המירבי הנתמך על ידי PSTN הוא 33,600 סיביות לשנייה, או 33.6Kbps. (Bit Rate)

תרשים 10.4 מציג את חיבורי PSTN.



תרשים 10.4 ציוד חיוג ותשתית WAN לחיבורי PSTN.

קישורים דיגיטליים ו- V.90

קצב הסיביות המירבי של תשתית הטלפונים הקיימת (PSTN), הוא פונקציה של טווח התדרים המועבר במרכזיות PSTN, ויחס אות-לרעש (Signal-to-Noise Ratio) של החיבור. מערכת הטלפונים האנלוגית של ימינו היא אנלוגית רק בלולאה המקומית (Local Loop), אותה קבוצת חוטים המקשרת את הלקוח למרכזת של חברת הטלפונים. מרגע שהאות האנלוגי מגיע למרכזת של חברת הטלפונים (PSTN Switch) הוא מומר לאות דיגיטלי. אותה המרה של אות, מאנלוגי לדיגיטלי, יוצרת על החיבור רעש המוכר בשם Quantization Noise.

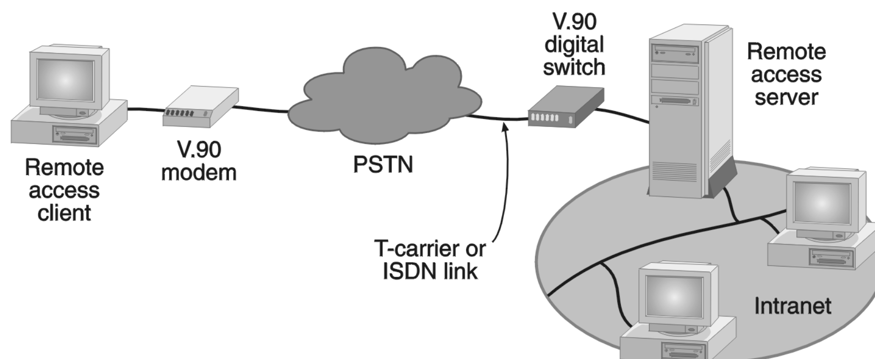
כאשר שרת RAS מחובר למשרד הראשי, באמצעות מרכזת דיגיטלית מבוססת T-Carrier או ISDN, ולא מרכזת PSTN אנלוגית, לא מתבצעת המרת האות מאנלוגי לדיגיטלי בעת ששרת גישה מרחוק שולח נתונים ללקוח הגישה מרחוק. כתוצאה מכך, לא נגרם רעש Quantization בנתיב היורד (Downstream) ללקוח הגישה מרחוק, ולכן יש יחס טוב יותר של אות-לרעש וקצב הסיביות המירבי גבוה יותר.

באמצעות טכנולוגיה חדשה זו, הנקראת V.90, לקוחות גישה מרחוק יכולים לשלוח נתונים בקצב של 33.6Kbps ולקבל נתונים בקצב 56Kbps. בצפון אמריקה קצב הסיביות הנכנס הגבוה ביותר הוא 53Kbps, בשל חוקי הוועדה הפדרלית לתקשורת (**F**ederal **C**ommunications **C**ommission - FCC).

כדי להשיג מהירויות של תקן V.90 חייבים להתמלא התנאים הבאים :

- במחשב לקוח הגישה מרחוק חייב להיות מותקן מודם התומך בתקן V.90.
- בשרת הגישה מרחוק חייבת להיות מרכזת דיגיטלית תומכת V.90 והוא חייב להשתמש בקישור דיגיטלי בהתקשרות למרכזת חברת הטלפונים (PSTN). הקישור יכול להיות מסוג ISDN או T-Carrier.
- אסור שתתבצענה המרות אות אנלוגי לאות דיגיטלי, במקום כלשהו בנתיב האות שבין שרת RAS ולקוח הגישה מרחוק.

תרשים 10.5 מציג חיבור PSTN מבוסס V.90 תקני.

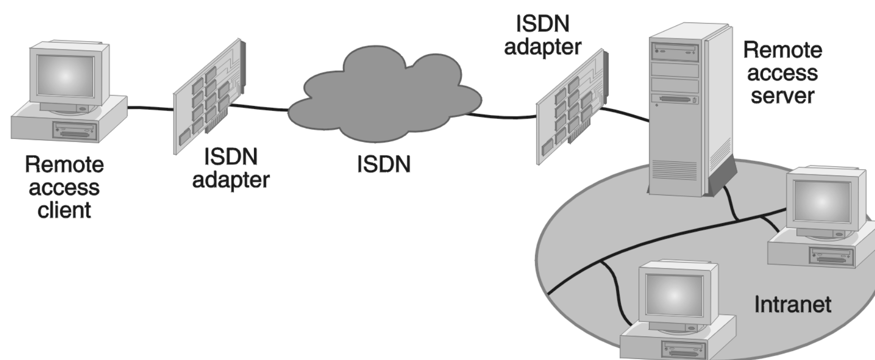


תרשים 10.5 ציוד חיוג ותשתית WAN לחיבורי PSTN.

ISDN

Integrated Services Digital Network - רשת דיגיטלית לשירותים משולבים, הידועה יותר בשם ISDN, היא קבוצה של מפרטים בינלאומיים לתחליף הדיגיטלי של PSTN. ISDN מאפשר לרשת דיגיטלית יחידה לטפל בקול, נתונים, פקס ושירותים נוספים על חיווט לולאה מקומית קיים. ISDN מתנהג כמו קו טלפון אנלוגי, מלבד העובדה שזו טכנולוגיה דיגיטלית, המאפשרת קצב העברת נתונים גבוה יותר ומשך התחברות קצר יותר. בקו ISDN יש מספר ערוצים B ; כל ערוץ מתפקד בקצב 64Kbps, ומאחר שהרשת היא דיגיטלית מקצה לקצה, לא מתבצעות המרות אנלוגי-דיגיטלי בשום שלב של ההתחברות.

ציוד חיוג כולל מתאם ISDN בלקוח הגישה מרחוק ובשרת הגישה מרחוק. לקוחות גישה מרחוק משתמשים בדרך כלל בקו בקצב בסיסי (**B**asic **R**ate **I**SDN - BRI), המכיל שני ערוצי 64Kbps, וארגונים גדולים משתמשים בדרך כלל בקו בקצב ראשי (PRI - **P**rimary **R**ate **I**SDN), המכיל 23 ערוצי 64Kbps. תרשים 10.6 מציג חיבור ISDN. לקו זה קוראים T1.



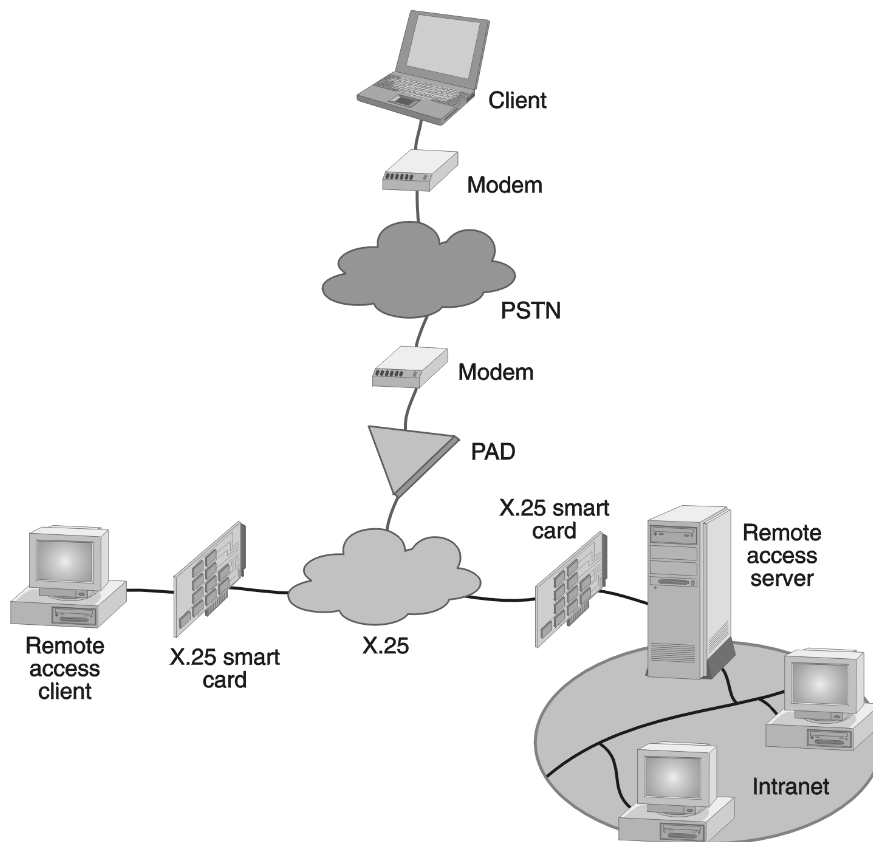
תרשים 10.6 ציוד חיוג ותשתית WAN לחיבוריות ISDN.

X.25

X.25 הוא תקן בינלאומי לשליחת נתונים באמצעות רשתות מיתוג מנות ציבורית (Public Packet Switching Networks). הגישה מרחוק של Windows 2000 תומכת בתקן X.25 בשתי דרכים :

- לקוח הגישה מרחוק תומך בשימוש בכרטיסים חכמים X.25 (X.25 Smart Cards) אשר מאפשרים חיבור ישיר לרשת נתוני X.25, ומשתמשים בפרוטוקול X.25 כדי ליצור חיבוריות, ולשלוח ולקבל נתונים. לקוח הגישה מרחוק גם תומך בחיוג לתוך מרכיב/מפרק מנות (**P**acket **A**ssembler/**D**isassembler - PAD) של נושא X.25 באמצעות מודם אנלוגי.
- שרת הגישה מרחוק של Windows 2000 תומך רק בחיבורים ישירים לרשתות X.25, תוך שימוש בכרטיס חכם X.25.

למידע נוסף אודות אופן הגדרת X.25 ו-PAD, פנה למערכת העזרה של שרת Windows 2000. תרשים 10.7 מציג חיבור X.25.



תרשים 10.7 ציוד חיוג ותשתית WAN לחיבורי X.25.

הערה כרטיס חכם X.25 הוא מתאם, המשתמש בפרוטוקול X.25, ויכול להתחבר ישירות לרשתות נתונים X.25 ציבוריות. אין קשר בין כרטיס חכם X.25 לכרטיס החכם המשמש לאימות ותקשורת מאובטחת.

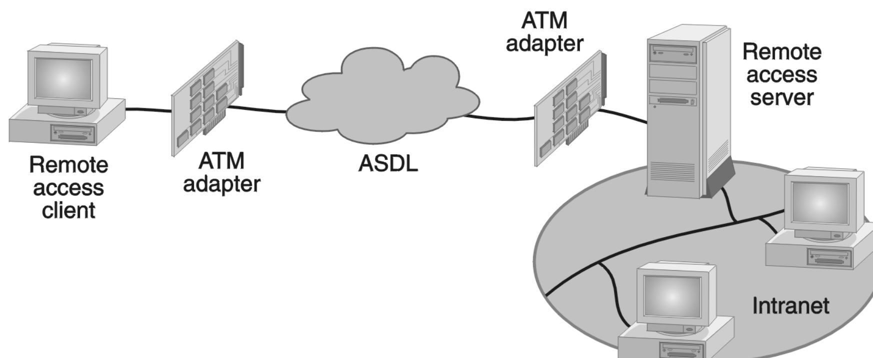
ATM over ADSL

ADSL (**A**symmetric **D**igital **S**ubscriber **L**ine), קו מנוי דיגיטלי א-סימטרי) הוא טכנולוגיית לולאה מקומית חדשה לעסקים קטנים ולמגזר הפרטי. למרות ש-ADSL מספק קצב שידור גבוה מאלה הזמינים באמצעות PSTN ו-ISDN, קצב השידור פנימה (Downstream, אל מחשב הלקוח) והחוצה (Upstream, ממחשב הלקוח) אינו זהה. חיבורי ADSL טיפוסיים מאפשרים קצב של 64Kbps (Kilo bit per second = Kbps) ממחשב הלקוח ו- 1.544Mbps (Mega bit per second = Mbps) אל מחשב הלקוח. הטבע הא-סימטרי של החיבור מתאים היטב לשימוש הטיפוסי באינטרנט. רוב רובם של משתמשי האינטרנט מקבלים מידע יותר מאשר שולחים מידע.

ציוד ADSL בסביבת Windows 2000 יכול להיתפס כממשק מתאם רשת Ethernet או כממשק חיוג. כאשר מתאם ADSL מופיע בתצורת ממשק רשת Ethernet, מתפקד חיבור ADSL באותו אופן בו מתבצע חיבור Ethernet לאינטרנט.

כאשר מתאם ADSL מופיע ב-Windows 2000 כממשק חיוג, מספק ADSL חיבור פיסי, ואילו מנות פרוטוקול LAN בודדות נשלחות, תוך שימוש במצב העברה א-סינכרוני (**A**synchronous **T**ransfer **M**ode - ATM). מתאם ATM עם יציאת ADSL מותקן גם בלקוח וגם בשרת הגישה מרחוק.

תרשים 10.8 מציג חיבור ATM על ADSL.



תרשים 10.8 ציוד חיוג ותשתית WAN לצורך חיבורי ATM על ADSL.

פרוטוקולים לגישה מרחוק

פרוטוקולים לגישה מרחוק מבקרים את תהליך יצירת ההתקשרות ואת מעבר הנתונים דרך קישורי WAN. מערכת ההפעלה ופרוטוקולי LAN, בהם נעשה שימוש בלקוחות ושרתי גישה מרחוק, מכתיבים באיזה פרוטוקול גישה מרחוק יכול הלקוח להשתמש.

קיימים שלושה סוגים של פרוטוקולי גישה מרחוק, הנתמכים על ידי הגישה מרחוק של Windows 2000 :

- ❖ **PPP** (**P**oin-to-**P**oint **P**rotocol) הוא קבוצת פרוטוקולים בחיוג בתקן תעשייתי, המספקת את מירב האבטחה, תמיכה בריבוי פרוטוקולים ופעילות משולבת (Interoperability).
- ❖ **SLIP** (**S**erial **L**ine **I**nternet **P**rotocol) משמש בעיקר בשרתי גישה מרחוק מיושנים (Legacy) ותומך רק ב-TCP/IP. שרת RAS של Windows 2000 אינו תומך בחיבורי SLIP בחיוג.
- ❖ Asynchronous NetBEUI, או AsyBEUI פרוטוקול הגישה מרחוק של Microsoft (Microsoft Remote Access Protocol) המשמש לקוחות גישה מרחוק מיושנים, הפועלים בסביבת מערכות הפעלה של Microsoft, כגון Windows NT גירסה 3.1, Windows for Workgroups, MS-DOS או LAN Manager.

פרוטוקולי LAN

פרוטוקולי LAN הם פרוטוקולים בהם משתמשים לקוחות גישה מרחוק, כדי לגשת למשאבים ברשת המחוברת לשרת RAS. הגישה מרחוק של Windows 2000 תומכת בפרוטוקולים TCP/IP, IPX, AppleTalk ו-NetBEUI.

אבטחת גישה מרחוק

הגישה מרחוק של Windows 2000 מציעה מיגוון רחב של מאפייני אבטחת מידע, כולל אימות משתמש מאובטח, אימות הדדי, הצפנת נתונים, חיוג חזרה (Callback), שיחה מזוהה (Caller ID) ונעילת חשבון גישה מרחוק.

אימות מאובטח של משתמש

אימות מאובטח של משתמש (Secure User Authentication) מושג באמצעות החלפה מוצפנת של נתוני המשתמש. דבר זה מתאפשר באמצעות השימוש בפרוטוקול PPP ובאחד מפרוטוקולי האימות הבאים :

- ❖ **E**xtensible **A**uthentication **P**rotocol - EAP
- ❖ **M**icro**s**oft **C**hallenge **H**andshake **A**uthentication **P**rotocol - MS-CHAP גירסאות 1 ו- 2.
- ❖ **C**hallenge **H**andshake **A**uthentication **P**rotocol - CHAP
- ❖ **S**hiva **P**assword **A**uthentication **P**rotocol - SPAP

שרת RAS יכול להיות מוגדר לדרוש שיטה של אימות מאובטח. אם לקוח הגישה מרחוק אינו יכול לבצע את האימות המאובטח הנדרש, ההתחברות אינה מתאפשרת.

Mutual Authentication

אימות הדדי (Mutual Authentication) מושג על ידי אימות שני קצוות ההתחברות, באמצעות החלפה מאובטחת של נתוני המשתמש. דבר זה מתאפשר תוך שימוש ב-PPP, יחד עם EAP-TLS (EAP-**T**ransport **L**evel **S**ecurity), או MS-CHAP גירסה 2. תוך כדי אימות הדדי, לקוח הגישה מרחוק מאמת את עצמו בשרת RAS, וכתגובה מאמת שרת RAS את עצמו אצל הלקוח.

ייתכן מצב בו שרת RAS אינו דורש אימות מלקוח הגישה מרחוק. אולם, במקרה של לקוח גישה מרחוק, הפועל בסביבת Windows 2000, ומוגדר רק עם EAP-TLS או MS-CHAP גירסה 2, כופה לקוח הגישה מרחוק אימות הדדי של הלקוח ושל השרת. אם שרת RAS אינו מגיב לבקשת האימות, מנותק החיבור על ידי הלקוח.

Data Encryption

הצפנת נתונים (Data Encryption) מצפינה את הנתונים הנשלחים בין לקוח הגישה מרחוק ושרת RAS. הצפנת נתוני גישה מרחוק מספקת הצפנה רק בקטע קישורי התקשורת שבין לקוח הגישה מרחוק ובין שרת RAS. אם יש צורך בהצפנה מקצה-לקצה (End-to-End Encryption), השתמש ב-IPSec כדי ליצור חיבור מוצפן מקצה-לקצה, לאחר שנוצר חיבור הגישה מרחוק.

הערה IPSec יכול גם לשמש להצפנת חיבורי VPN באמצעות L2TP (**L**ayer **2** **T**unneling **P**rotocol). למידע נוסף פנה לשיעור 4.

הצפנת נתונים בחיבורי גישה מרחוק מבוססת על מפתח הצפנה סודי, הידוע לשרת RAS וללקוח הגישה מרחוק. מפתח סודי משותף זה נוצר בעת תהליך אימות המשתמש.

הצפנת נתונים בקישורי גישה מרחוק בחיוג, זמינה כאשר משתמשים ב-PPP יחד עם EAP-TLS או MS-CHAP. שרת RAS יכול להיות מוגדר כך שידרוש הצפנת נתונים. אם לקוח הגישה מרחוק אינו מבצע את ההצפנה הנדרשת, ניסיון החיבור יידחה.

לקוחות ושרתי גישה מרחוק של מערכות ההפעלה Windows 95/98/NT4/2000 תומכים כולם בפרוטוקול ההצפנה של Microsoft, MPPE (**M**icrosoft **P**oin-to-**P**oint **E**ncription Protocol). MPPE משתמש במצפין RC4 של RSA (**R**ivest-**S**hamir-**A**dleman) ובמפתחות סודיים בני 40, 56 או 128 סיביות. מפתחות MPPE נוצרים מתהליכי אימות המשתמש של EAP-TLS ו-MS-CHAP.

Callback

באמצעות חיוג חזרה (Callback), שרת RAS מתקשר אל הלקוח, לאחר שנתוני המשתמש אומתו ואושרו. חיוג חזרה יכול להיות מוגדר בשרת, כך שיתקשר אל לקוח הגישה מרחוק למספר המצוין על ידי המשתמש בעת תהליך יצירת הקשר. דבר זה מאפשר ללקוח נייד לחייג לרשת הארגון, ולדאוג לכך ששרת RAS יתקשר אליו חזרה למיקומו הנוכחי, (ובכך לחסוך את עלויות השיחה מהמשתמש). חיוג חזרה יכול גם להיות מוגדר כך, שכדי לחזור ולהתקשר אל לקוח הגישה מרחוק המסוים הזה, תמיד יחויג מספר קבוע, שזו הצורה המאובטחת של חיוג חזרה.

Caller ID

שיחה מזוהה (Caller ID) יכולה לשמש כדרך לוודא שהשיחה הנכנסת מגיעה ממקור מסוים. שיחה מזוהה מוגדרת כחלק ממאפייני החיוג פנימה (Dial-in Properties) של חשבון המשתמש. אם המספר המזוהה של השיחה הנכנסת מאותו משתמש אינו תואם את הגדרות Caller ID בחשבון שלו, החיבור יידחה.

שיחה מזוהה מחייבת שקו הטלפון, ממנו מתבצע החיוג, רשת הטלפונים, קו הטלפון של שרת RAS של Windows 2000 ומנהלי ההתקנים עבור ציוד החיוג של Windows 2000, כולם כאחד יתמכו בשירות השיחה המזוהה. אם לחשבון המשתמש מוגדרת שיחה מזוהה, אך זיהוי השיחה אינו מועבר לשרת RAS - החיבור יידחה.

שיחה מזוהה היא מאפיין שנועד לספק רמה גבוהה יותר של אבטחה לרשתות התומכות במשתמשי חיוג. החיסרון בהגדרת שיחה מזוהה נעוץ בכך, שהמשתמש חייב להתקשר תמיד מאותו קו טלפון. זהו חיסרון דומה לזה שבהגדרת חיוג חזרה למספר טלפון מסוים.

נעילת חשבון גישה מרחוק

מאפיין נעילת חשבון גישה מרחוק (Remote Access Account Lockout) משמש להגדרת מספר הפעמים, בהן מורשה ניסיון אימות גישה מרחוק להיכשל מול חשבון משתמש חוקי, עד שגישתו מרחוק של המשתמש תידחה. נעילת חשבון גישה מרחוק חשובה ביותר עבור התחברויות VPN באמצעות האינטרנט. משתמשים בעלי כוונת-זדון ברשת האינטרנט יכולים לנסות ולהתחבר לרשת האינטראנט של הארגון, על ידי שליחת נתוני משתמש (שם משתמש חוקי וסיסמה משוערת), בעת תהליך אימות של התחברות VPN. בעת השימוש בהתקפת מילון (Dictionary Attack), שולח המתקיף מאות ואף אלפי נתוני משתמש, תוך שימוש ברשימת סיסמאות המבוססת על מילים או משפטים מוכרים. כאשר מאפיין נעילת חשבון גישה מרחוק פעיל, נבלם ניסיון מתקפת מילון לאחר מספר ניסיונות כושלים.

מאפיין נעילת חשבון גישה מרחוק אינו מבחין בין משתמשים בעלי כוונת-זדון, המנסים לחדור לרשת האינטראנט, לבין משתמשים חוקיים המנסים לבצע גישה מורשית לחשבונם, אך שכחו את סיסמתם הנוכחית. משתמשים אשר שכחו את סיסמתם, נוהגים לנסות מספר פעמים, מספר סיסמאות שונות. בהתאם למספר הניסיונות המוגדר ולהגדרת MaxDenial, ייתכן שחשבונם יינעל בפניהם.

אם אתה מפעיל את מאפיין נעילת חשבון הגישה מרחוק, יכול משתמש הפועל בכוונות-זדון לנעול במכוון חשבונות, על ידי ניסיונות חוזרים ונשנים להיכנס באמצעות חשבון זה, עד שהחשבון יינעל, ועל ידי כך למנוע מהמשתמש המורשה להיכנס למערכת.

כמנהל הרשת עליך לקבוע שני משתנים לנעילת חשבון משתמש בגישה מרחוק:

- **מספר הניסיונות הכושלים עד שניסיונות עתידיים יידחו** – לאחר כל ניסיון כושל, מקודם מונה כשלונות התחברות עבור חשבון המשתמש. אם המונה מגיע למירב הניסיונות המוגדר בו, יידחו ניסיונות עתידיים לכניסה למערכת. אימות מוצלח של נתוני הלקוח מאפס את מונה כשלונות ההתחברות של החשבון, כאשר הערך בו נמוך מערכו המירבי המוגדר. במילים אחרות, מונה כשלונות ההתחברות אינו ממשיך למנות מעבר לניסיון התחברות מוצלח.
- **מדי כמה זמן מונה הניסיונות הכושלים מאופס** – עליך לאפס מדי זמן את מונה כשלונות ההתחברות, כדי למנוע נעילות שלא בכוונה, הנובעות משגיאות המשתמש בעת הקלדת הסיסמה.

ניהול גישה מרחוק

כאשר אתה מנהל גישה מרחוק, עליך לקחת בחשבון מיגוון גורמים, כגון היכן יש לאחסן את נתוני חשבונות המשתמשים, כיצד יוקצו כתובות ללקוחות הגישה מרחוק ולמי מותר ליצור חיבורי גישה מרחוק. ניהול גישה מרחוק כולל ניהול משתמשים, כתובות, גישה ואימות.

ניהול משתמשים

במקום לנהל חשבונות משתמש נפרדים עבור אותם משתמשים בשרתים שונים, ולנסות לשמור על החשבונות עדכניים במידה שווה, יוצרים רוב מנהלי הרשתות מסד נתוני חשבון ראשי (Master Account Database), הנשמר במחסן Active Directory או בשרת RADIUS. דבר זה מאפשר לשרת RAS לשלוח נתוני אימות להתקן אימות מרכזי.

ניהול כתובות

בהתחברויות PPP, ‏IP, ‏IPX ו-AppleTalk יש להקצות את נתוני המיעון (Addressing Information) ללקוח הגישה מרחוק תוך כדי יצירת ההתחברות. שרת RAS של Windows 2000 חייב להיות מוגדר להקצאת כתובות IP, כתובות רשת וצומת IPX, או כתובות רשת וצומת AppleTalk.

ניהול גישה

ב-Windows 2000 חיבורי גישה מרחוק מתקבלים בהתבסס על מאפייני החיוג שבחשבון המשתמש ומדיניות הגישה מרחוק. מדיניות גישה מרחוק היא קבוצת תנאים ונתוני התחברות, המגדירים את אופי החיבור מבחוץ ואת קבוצת המכולות הנכפית על ההתחברות. מדיניות גישה מרחוק יכולה לשמש לאכיפת נתוני התחברות, כגון משך זמן מירבי להתחברות, משך זמן ללא פעילות שאחריו תנותק ההתחברות, שיטות אימות נדרשות, הצפנה נדרשת וכדומה.

כאשר מגדירים מספר מדיניות (Policies) גישה מרחוק, ניתן להחיל על לקוחות גישה מרחוק שונים, קבוצות שונות של הגדרות, או שניתן לקבוע דרישות שונות לאותו לקוח גישה מרחוק, בהתאם לפרמטרים שונים, המזוהים בעת ניסיון ההתחברות שלו.

לדוגמה, מיגוון מדיניות גישה מרחוק יכולות לשמש לצרכים הבאים :

- ❖ אם חשבון המשתמש שייך לקבוצה מסוימת - אַפשר (Enable) או דְחה (Deny) את החיבור.
- ❖ בהתאם לשיוכו לקבוצת משתמשים, הגדר למשתמש ימים ושעות שונות, בהן יוכל לבצע התחברות.
- ❖ הגדר שיטות אימות שונות ללקוחות גישה מרחוק בחיוג וללקוחות גישה מרחוק VPN.
- ❖ קבע הגדרות אימות או הצפנה שונות עבור חיבורי PPTP או חיבורי L2TP.
- ❖ קבע טווחי זמן שונים עד לסיומו של חיבור למשתמשים שונים, בהתבסס על חברות בקבוצות שונות.
- ❖ שלח ללקוח RADIUS מאפייני RADIUS לגישה לרשת ייחודיים-לשרת.

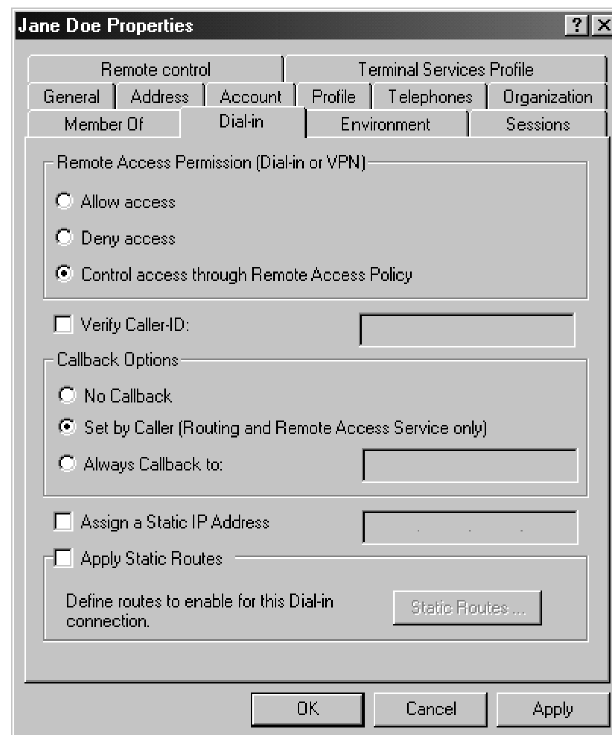
כאשר יש לך מספר שרתי גישה מרחוק של Windows 2000, או שרתי VPN, בהם אתה מעוניין להשתמש כדי לרכז קבוצה של מדיניות, תוכל להגדיר מחשב Windows 2000 לפעול עם IAS (**I**nternet **A**uthentication **S**ervice) ואז להגדיר כל שרת גישה מרחוק או שרת VPN כלקוח RADIUS בשרת IAS.

גם RRAS של Windows 2000 וגם IAS של Windows 2000 משתמשים במדיניות הגישה מרחוק, כדי לקבוע האם לקבל או לדחות ניסיונות התחברות. במקרה של RRAS, מדיניות גישה מרחוק מנוהלת באמצעות תוסף התוכנה Routing and Remote Access, ואילו במקרה של IAS מנוהלת מדיניות גישה מרחוק באמצעות תוסף התוכנה Internet Authentication Service.

באמצעות מדיניות גישה מרחוק אתה יכול לאפשר גישה מרחוק, על ידי הגדרת חשבון משתמש או על ידי הגדרת מדיניות גישה מרחוק ייחודית.

גישה באמצעות חשבון משתמש

חשבון המשתמש (User Account) במחשב העומד בפני עצמו, או בשרת מבוסס Active Directory, כולל קבוצת מאפייני חיוג פנימה (Dial-in Properties) בהם נעשה שימוש כאשר מתקבל או נדחה ניסיון התחברות של המשתמש. בשרת עצמאי (Stand-alone Server) תוכל להגדיר את מאפייני החיוג בכרטיסיה Dial-In, שבמאפייני המשתמש בתוסף התוכנה Local Users and Groups. במחשב מבוסס Active Directory תוכל לקבוע את מאפייני החיוג של מאפייני חשבון המשתמש בתוסף התוכנה של Active Directory Users And Computers, כפי שנראה בתרשים 10.9.



תרשים 10.9 הגדרות חיוג פנימה בשירותי Active Directory עבור משתמשת בשם Jane Doe.

הכרטיסיה Dial-In כוללת מספר אפשרויות: הרשאות גישה מרחוק בחיוג או VPN (Remote Access Permissions (Dial-in or VPN)), וידוא שיחה מזוהה (Verify Caller ID), אפשרויות חיוג חזרה (Callback Options), הקצאת כתובת IP קבועה (Assign A Static IP Address) והחלת נתיבים קבועים (Apply Static Routes).

הערה במקרה של חשבון משתמש ב-Windows NT 4.0 Domain **או** Windows 2000 Mixed Mode Domain, **יהיו זמינות רק האפשרויות** Allow Access **ו-** Deny Access **בחלק** Remote Access Permissions (Dial-in or VPN), **והאפשרויות שבחלק** Callback Options**.**

Remote Access Permissions (Dial-in or VPN)

מאפיין זה מגדיר האם הגישה מרחוק תוגדר באופן חד משמעי כאפשרית, בלתי אפשרית או שהיא תיקבע באמצעות מדיניות גישה מרחוק. אם הגישה מאופשרת באופן חד משמעי, עדיין יכולים תנאי מדיניות הגישה מרחוק, מאפייני חשבון המשתמש או מאפייני פרופיל לגרום לדחייה של ניסיון ההתחברות. האפשרות Control access through Remote Access Policy זמינה רק בחשבון משתמש ב-Windows 2000 Navite Mode או לחשבונות מקומיים בשרתי גישה מרחוק Windows 2000, הפועלים כשרתים עצמאיים.

כברירת מחדל, בחשבונות Administrator ו-Guest בשרת גישה מרחוק עצמאי או ב-Windows 2000 Native Mode Domain האפשרות Control access through Remote Access Policy מסומנת, ואילו ב-Windows 2000 Mixed Mode Domain הם מוגדרים כ-Deny access. חשבונות חדשים הנוצרים בשרת RAS עצמאי או ב-Windows 2000 Native Mode Domain מוגדרים עם האפשרות Control access through Remote Access Policy. חשבונות חדשים הנוצרים ב-Windows 2000 Mixed Mode Domain מוגדרים כ- Deny access.

Verify Caller ID

אם אפשרות זו מסומנת, מוודא השרת את מספר הטלפון של המתקשר. אם מספר הטלפון של המתקשר אינו תואם למספר הטלפון המוגדר, ניסיון ההתחברות נכשל.

שירות השיחה המזוהה צריך להיות נתמך על ידי המתקשר, מערכת התקשורת שבין המתקשר ושרת הגישה מרחוק ועל ידי שרת הגישה מרחוק עצמו. שיחה מזוהה בשרת הגישה מרחוק כוללת ציוד מענה לשיחה, התומך בהעברת נתוני שיחה מזוהה ובמנהל התקן מתאים מותקן ב-Windows 2000, התומך בהעברת נתוני השיחה המזוהה לשרת הגישה מרחוק.

אם הגדרת מספר טלפון עבור משתמש, ולא קיימת תמיכה בהעברת נתוני השיחה המזוהה מהמתקשר לשרת הגישה מרחוק, ניסיון ההתחברות ייכשל.

Callback Options

כאשר אפשרות זו פעילה, מתקשר השרת חזרה אל המתקשר תוך תהליך יצירת החיבור, למספר אותו קובע המתקשר, או למספר טלפון המוגדר מראש על ידי מנהל הרשת.

אם חשבון המשתמש הוא ב-Windows 2000 Native Mode Domain, יכול מספר הטלפון לחיוג חזרה להיות באורך של עד 128 תווים. אם חשבון המשתמש הוא בשרת RAS הפועל בשרת Windows 2000 עצמאי, ב-Windows NT 4.0 Domain או בסביבת ב-Windows 2000 Mixed Mode Domain, יכלול המספר 24 עד 48 תווים, הודות למבנה הדחוס של אחסון מספרי חיוג חזרה (Callback numbers). מספרי חיוג חזרה עשויים להיות ארוכים, במקרה של שיחות בינלאומיות, או במקרה של חיוג באמצעות קודי חיוג נוספים, כגון כרטיסי חיוג.

Assign a Static IP Address

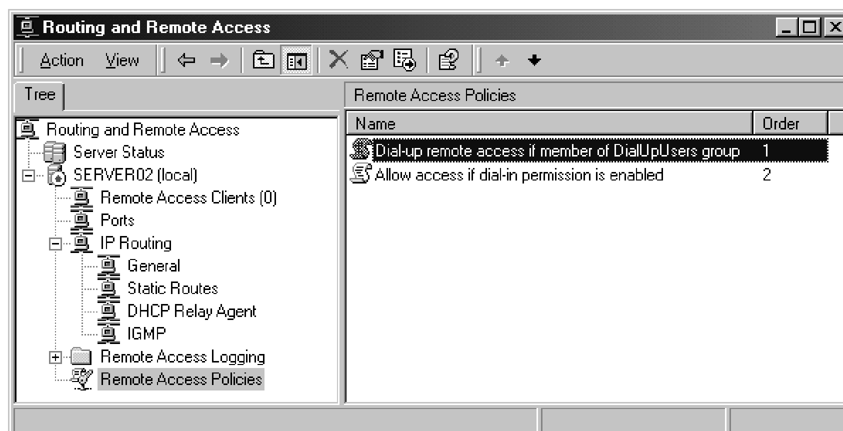
כאשר אפשרות זו פעילה, ניתן להגדיר כתובת IP מסוימת למשתמש, כשנוצר חיבור.

Apply Static Routes

אם אפשרות זו פעילה, תוכל לקבוע רצף נתיבי IP קבועים, הנוספים לטבלת הניתוב בשרת הגישה מרחוק כשנוצר החיבור. הגדרה זו נועדה עבור חשבונות המשתמש, בהם משתמשים נתבי Windows 2000 לניתוב חיוג-על-פי-דרישה.

גישה באמצעות מדיניות

המודל הניהולי של גישה באמצעות מדיניות נועד עבור שרתי RAS של Windows 2000, שהם שרתים חברים ב-Windows 2000 Native Mode Domain. לניהול גישה מרחוק באמצעות מדיניות, סמן את לחצן האפשרויות Control access through Remote Access Policy (בכרטיסיה Dial-in, שבתיבת הדו-שיח Properties של המשתמש) בכל חשבונות המשתמשים (ראה תרשים 10.9), ואז קבע את המדיניות החדשה, המאפשרת או דוחה גישה, בהתאם לצרכיך. מדיניות גישה מרחוק מוגדרת באמצעות ספק אימות (Authentication Provider) של RRAS או של RADIUS. תרשים 10.10 מראה את הצומת Remote Access Policy בתוסף התוכנה Routing and Remote Access.



תרשים 10.10 הצומת Remote Access Policy בתוסף התוכנה Routing and Remote Access, כאשר בחלונית הפרטים מופיעות שתי רשומות של מדיניות.

הצומת Remote Access Policy מופיע בתוסף התוכנה Routing and Remote Access, כאשר ספק האימות (Authentication Provider) מוגדר כ- Windows Authentication. כאשר ספק האימות מוגדר כ- RADIUS Authentication (ראה תרשים 10.2), הצומת אינו מופיע. במקום זאת, המדיניות מוגדרות מממשק ספק האימות של RADIUS.

אם מחשב שרת הגישה מרחוק הוא חבר ב-Windows NT 4.0 Domain או ב-Windows 2000 Mixed Mode Domain ואתה מעוניין לנהל את הגישה באמצעות מדיניות, סמן את לחצן האפשרויות Allow access (בכרטיסיה Dial-in, שבתיבת הדו-שיח Properties של המשתמש) בכל חשבונות המשתמשים. אז, הסר את מדיניות ברירת המחדל Allow access if Dial-in Permission is enabled, וצור מדיניות חדשה המאפשרת או דוחה את אפשרות הגישה. חיבור שאינו תואם מדיניות גישה כלשהי יידחה, אפילו אם לחצן Allow access מסומן בחשבון המשתמש.

שימוש נפוץ בגישה מבוססת-מדיניות הוא לאפשר גישה דרך חברות בקבוצה. לדוגמה, צור קבוצת Windows 2000 בשם, כגון DialUpUsers ובה חברים אותם משתמשים המורשים לבצע גישה מרחוק.

כדי ליצור שרת גישה מרחוק, המאפשר רק חיבורי גישה מרחוק בחיוג, צור מדיניות גישה מרחוק חדשה בעלת שם תיאורי, כגון Dial-up remote access if member of DialUpUsers, החל אותה על הקבוצה DialUpUsers ואז מחק את מדיניות הגישה מרחוק שבברירת המחדל, זו הנקראת Allow access if Dial-in Permission is enabled.

תהליך ניסיון התחברות

כאשר משתמש מנסה להתחבר, ניסיון ההתחברות מתקבל, או נדחה, בהתאם ללוגיקה הבאה:

1. נבדקת המדיניות הראשונה ברשימת מדינויות הגישה מרחוק. אם לא קיימות מדינויות גישה מרחוק - דחה את ניסיון ההתחברות.
2. אם תנאי כלשהו של המדיניות אינו תואם לניסיון ההתחברות, עבור למדיניות הבאה. אם לא קיימות מדינויות חדשות - דחה את ניסיון ההתחברות.
3. אם כל תנאי המדיניות תואמים את ניסיון ההתחברות, בדוק את הגדרות הרשאת גישה מרחוק עבור המשתמש המנסה לבצע את ההתחברות.

❖ אם האפשרות Deny Access מסומנת, דחה את ניסיון ההתחברות.

❖ אם האפשרות Allow Access מסומנת, החל את מאפייני חשבון המשתמש ואת מאפייני הפרופיל.

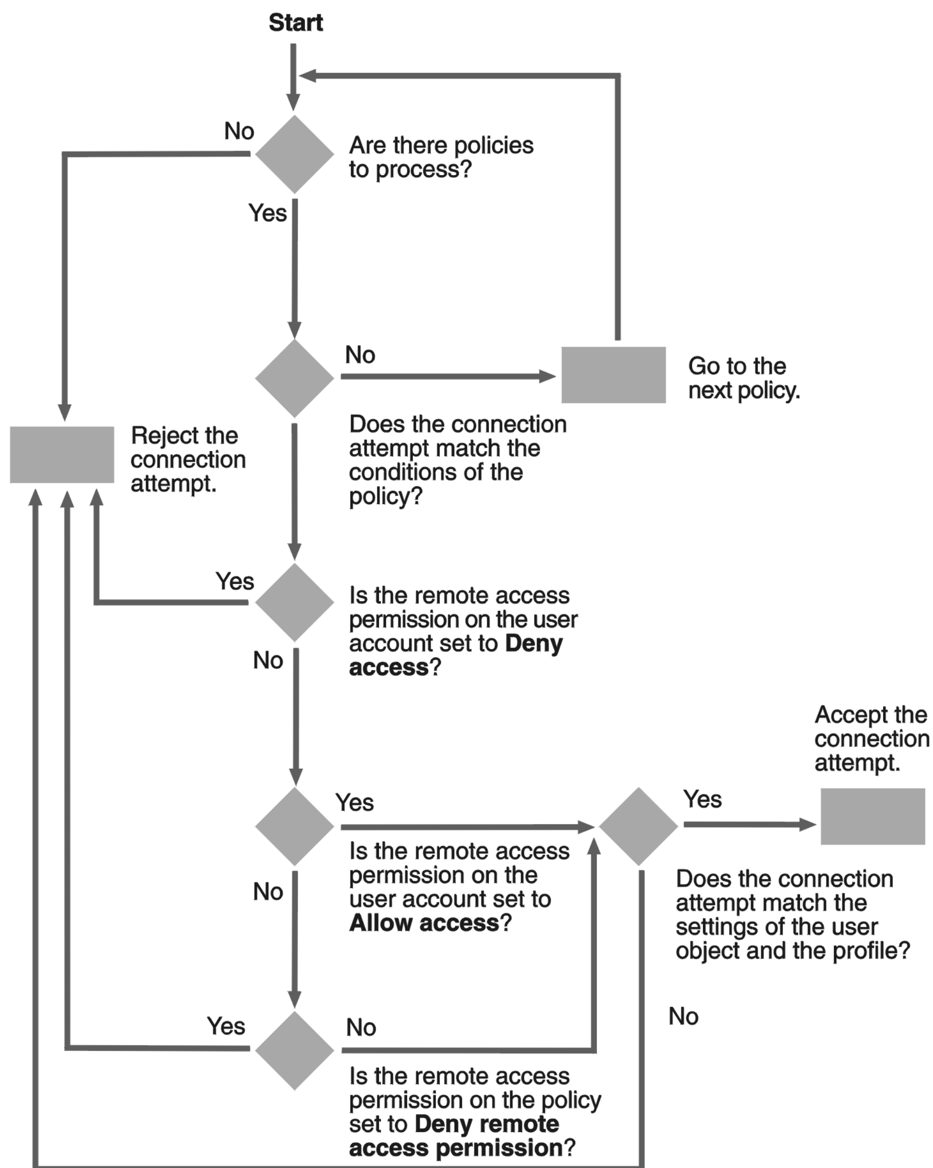
- אם ניסיון ההתחברות אינו תואם את ההגדרות של מאפייני חשבון המשתמש ואת מאפייני הפרופיל - דחה את ניסיון ההתחברות.
- אם ניסיון ההתחברות תואם את ההגדרות של מאפייני חשבון המשתמש ואת מאפייני הפרופיל - אשר את ניסיון ההתחברות.

❖ אם נבחרה האפשרות Control access through Remote Access Policy, בדוק את הגדרות הרשאת גישה מרחוק עבור המדיניות.

- אם נבחרה האפשרות Deny Remote Access Permission - דחה את ניסיון ההתחברות.
- אם נבחרה האפשרות Grant Remote Access Permission - החל את מאפייני חשבון המשתמש ואת מאפייני הפרופיל.

❖ אם ניסיון ההתחברות אינו תואם את הגדרות מאפייני חשבון המשתמש ומאפייני הפרופיל - דחה את ניסיון ההתחברות.

❖ אם ניסיון ההתחברות תואם את הגדרות מאפייני חשבון המשתמש ומאפייני הפרופיל - אשר את ניסיון ההתחברות.



תרשים 10.11 השימוש במדיניות גישה מרחוק והגדרות חשבון משתמש לאישור ניסיון התחברות.

ניהול נעילת חשבון

את מאפיין נעילת חשבון גישה מרחוק (Remote Access Account Lockout) מגדירים על ידי שינוי ערכים ברישום המערכת (Registry) של Windows 2000, המספק את שירותי האימות. אם שרת RAS מוגדר גם כספק אימות מסוג Windows Authentication, שנה את רישום המערכת במחשב זה. אם שרת RAS מוגדר לשימוש בספק אימות RADIUS (RADIUS Authentication) ונעשה שימוש גם ב-IAS של Windows 2000, שנה את רישום המערכת במחשב שהוא שרת IAS.

כדי לאפשר נעילת חשבון, עליך לשנות את ערך הרשומה MaxDenials ברישום המערכת HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout) לערך 1 או גבוה יותר. הרשומה MaxDenials מתארת את מספר הניסיונות הכושלים המירבי האפשרי לפני שהחשבון ננעל. כברירת מחדל מוגדר ערך MaxDenials כ-0 (אפס), מה שמצביע על כך שאפשרות נעילת החשבון אינה פעילה. המפתח AccountLockout נוצר כאשר מאופשר שירות RRAS.

כדי להתאים את משך הזמן לפני שמונה הניסיונות הכושלים יאופס מחדש, עליך להגדיר את את ערך הרשומה ResetTime (Mins) שברישום המערכת (במפתח כפי שמוזכר קודם לכן), למספר הדקות המבוקש. כברירת מחדל מוגדר לרשומה ResetTime (Mins) הערך ההקסה-דצימלי b40, או 2,880 דקות (שהן 248 שעות).

כדי לאפס באופן ידני חשבון משתמש שננעל, לפני שמונה האיפוס האוטומטי עושה זאת, מחק את מפתח המשנה הבא, המקביל לשם חשבון המשתמש HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess\Parameters\AccountLockout\<*domain_name:user_name*>.

הערה למאפיין נעילת חשבון גישה מרחוק (Remote Acce Account Lockout) אין כל קשר להגדרה Account is locked out שבכרטיסיה Account בתיבת הדו-שיח Properties של המשתמש, או למדיניות ניהול נעילת חשבונות שבמדינויות הקבוצתיות (Group Policies) של Windows 2000.

ניהול אימות

שרת הגישה מרחוק יכול להיות מוגדר לשימוש בספק אימות Windows או RADIUS. תרשים 10.2 מציג את המקום בו מתבצעת הבחירה ביניהם, בתוסף התוכנה Routing and Remote Access.

Windows Authentication

אם Windows נבחרה כספק האימות, אזי נתוני המשתמש (User Credentials), הנשלחים על ידי לקוחות שמנסים לבצע התחברות בגישה מרחוק, מאומתים באמצעות מנגנון אימות רגיל של Windows.

אם שרת הגישה מרחוק הוא שרת-חבר (Member Server) ב-Windows 2000 Native\Mixed Mode Domain, והוא מוגדר לאימות Windows, חשבון המחשב עבור מחשב שרת RAS חייב להיות חבר בקבוצת האבטחה (RAS and IAS (Security Group Servers. הגדרת חברות ניתן להשלים באמצעות תוסף התוכנה Active Directory Users and Computers, כדי להוסיף את המחשב לקבוצת האבטחה RAS and IAS Servers שבמכולה Users. פקודת שורת הפקודה netsh יכולה גם היא לשמש לשם כך. לדוגמה, כדי להוסיף שרת ששמו RAS1 לקבוצת האבטחה RAS and IAS Servers ב-domain בשם microsoft.com, פתח חלון שורת פקודה והפעל את תוכנית השירות Net Shell על ידי הקלדת הפקודה netsh והקשה על Enter. כעת, כשאתה פועל בתוכנית השירות Net Shell, הקלד את הפקודה **add registeredserver domain=microsoft.com server=ras1**. אם המשתמש המתקין את RRAS הוא מנהל (Administrator), מוסף חשבון המחשב באופן אוטומטי לקבוצת האבטחה RAS and IAS Servers בעת התקנת RRAS.

RADIUS Authentication

אם ספק האימות הנבחר והמוגדר בשרת הגישה מרחוק הוא RADIUS, נשלחים נתוני המשתמש ופרמטרים של בקשת ההתחברות כסדרת הודעות-בקשה של RADIUS (RADIUS Request Messages) לשרת RADIUS, כגון מחשב מבוסס שרת Windows 2000 ו-IAS.

שרת RADIUS מקבל בקשת התחברות של משתמש משרת RAS ומאמת את הלקוח מול מסד נתוני האימות שלו. שרת RADIUS יכול גם להחזיק במסד נתונים מרכזי של מאפייני משתמש רלוונטיים נוספים. בנוסף למענה *כן* או *לא* פשוט לבקשת אימות, יכול שרת RADIUS גם להודיע לשרת RAS אודות פרמטרים נוספים הקשורים במשתמש זה, כגון משך זמן מירבי של התחברות, הקצאת כתובת IP קבועה וכדומה.

RADIUS מסוגל להגיב לבקשות אימות, בהתבסס על מסד הנתונים שלו, או שהוא יכול להוות חזית עבור שרת מסד נתונים אחר, כגון שרת ODBC (**O**pen **D**ata**b**ase **C**onnectivity) גינרי או Windows 2000 Domain Controller, היכול להיות אותה מכונה בה פועל שרת RADIUS, או במקום מרכזי אחר כלשהו. בנוסף, שרת RADIUS יכול לשמש גם כלקוח Proxy לשרת RADIUS מרוחק.

פרוטוקול RADIUS מפורט במסמך RFC 2139. למידע נוסף אודות תרחישי אימות של שרת RAS כלקוח RADIUS, פנה למערכת העזרה של Windows 2000 Server.

הערה כאשר הם מוגדרים לאימות Windows, גם RRAS וגם IAS מבצעים את אותו תהליך לאספקת אימות ואישור של בקשות חיבור.

ניהול חשבונות של Windows ו-RADIUS

תוכל לבחור באפשרות Windows Accounting, RADIUS Accounting או None בכרטיסיה Security שבתיבת הדו-שיח Properties של שרת הגישה מרחוק. כאשר האפשרות Windows Accoounting פעילה, תומך שרת גישה מרחוק המבוסס Windows 2000 בניהול יומן רישום נתוני ניהול חשבונות (Accounting Information Logging) לחיבורי שרת גישה מרחוק בקבצי יומן מקומיים. יומנים אלה נפרדים מרישום האירועים שברישום יומן המערכת (System Event Log). רישום יומן ניהול חשבונות, יעיל במיוחד לשם טיפול בתקלות במדיניות הגישה מרחוק. נתוני ניהול החשבונות מאוחסנים בקובץ יומן, אחד או יותר, שאת תצורתו ניתן להגדיר, בתיקיה %systemroot%\System32\LogFiles. קבצי היומן נשמרים במבנה IAS 1.0 או ODBC - מה שאומר שכל יישום מסד נתונים התואם ODBC יכול לקרוא קובץ יומן באופן ישיר, לשם ניתוחו.

שרת גישה מרחוק מבוסס Windows 2000 תומך גם בניהול יומן נתוני ניהול חשבונות עבור חיבורי שרתי גישה מרחוק בשרת RADIUS, כאשר שירות אימות וחישבון של RADIUS פעיל ומאופשר. יומן זה נפרד מהאירועים הנרשמים ביומן אירועי המערכת. אם שרת ה-RADIUS שלך הוא מחשב Windows 2000 המפעיל את IAS, אזי נתוני ניהול החשבונות נרשמים בקבצי היומן הנשמרים בשרת IAS.

תרגיל 2: הגדרה וניטור חיבור RAS (גישה מרחוק מאובטחת)

תרגיל זה יש להשלים במחשב Server01 ובמחשב Server02.

הליך 1: אישור ודחייה של גישה בחיוג

בהליך זה תאפשר ותדחה באופן בררני גישה מרחוק של חשבונות משתמשים. השלם הליך זה במחשב Server01.

1. פתח את תוסף התוכנה של Active Directory Users and Computers.

   חלון תוסף התוכנה של Active Directory Users and Computers ייפתח.
2. בחלון Tree לחץ על Sales OU. האובייקטים של Sales OU יופיעו בחלונית הפרטים.
3. לחץ לחיצה כפולה על Jane Doe. תיבת הדו-שיח Jane Doe Properties תופיע.
4. בחר בכרטיסיה Dial-in. יופיעו הגדרות החיוג פנימה של Jane Doe.
5. לחץ על לחצן האפשרויות Allow access, ולחץ OK.
6. לחץ לחיצה כפולה על John Smith בחלונית הפרטים ובחר בכרטיסיה Dial-in. יופיעו הגדרות החיוג פנימה של John Smith.

7. ודא כי לחצן האפשרויות Control access through Remote Access Policy מסומן, ולחץ OK.
8. בחלון Tree לחץ על המכולה Users. האובייקטים שבמכולה Users יופיעו בחלונית הפרטים.
9. עבור למאפייני החיוג פנימה של המשתמש Bob Train.
10. לחץ על לחצן האפשרויות Deny Access, ולחץ OK.
11. סגור את Active Directory Users and Computers.

הליך 2: אפשור ניהול חשבונות והגדרת ניהול יומן בשרת RRAS

בהליך זה תגדיר את שרת RRAS לרישום יומן ניהול חשבונות של Windows ויומן אירועים. השלם הליך זה במחשב Server01.

1. שחזר את חלון תוסף התוכנה Routing and Remote Access.
2. בחלון Tree לחץ על Remote Access Logging.
3. בחלונית הפרטים, לחץ לחיצה כפולה על Local File.

   תיבת הדו-שיח Local File Properties תופיע.
4. סמן את תיבת הסימון Log Authentication Requests Access Accept או את תיבת הסימון Access Reject - Recommended.
5. לחץ OK.
6. בחלון Tree לחץ על Server01 (Local).
7. פתח את תפריט Action ובחר Properties.

   תיבת הדו-שיח Server01 (Local) Properties תופיע.
8. בחר בכרטיסיה Event Logging.
9. לחץ על לחצן האפשרויות Log the maximum amount of information וסמן את תיבת הסימון Enable Point-to-Point Protocol (PPP) logging.
10. לחץ OK. תיבת ההודעה Routing and Remote Access תופיע ותבקש לאתחל את השירות.
11. לחץ Yes. מספר תיבות הודעה יופיעו בעת ששירות הניתוב והגישה מרחוק נעצר ומאותחל.

הליך 3: הגדרת לקוח חיוג וגישה לשרת RRAS (אופציונלי)

בהליך זה תגדיר את שרת Server02 שישמש כלקוח חיוג. כדי להשלים את תרגיל זה חייב להיות מודם מותקן ומוגדר כהלכה במחשב Server02.

1. לפני הפעלת המחשב Server02, נתק ממנו את כבל הרשת.
2. הפעל את המחשב Server02.
3. במסך הכניסה, פתח את תיבת הרשימה הנפתחת Logon to, בחר SERVER02 (This computer) ואז היכנס למערכת בשם משתמש Administrator ועם הסיסמה password.
4. לחץ Start, הצבע על Settings ולחץ על Network and Dial-up connections.

   חלון Network and Dial-up connections יופיע. שים לב שהסמל של Local Area Connection מכיל סימן X אדום. זאת, כיון שניתקת את קישור הרשת המקומי (Local Area Connection) לפני תחילת הליך זה.
5. לחץ לחיצה כפולה על הסמל Make New Connection.

   האשף Network Connection יופיע.
6. לחץ Next. יופיע המסך Network Connection Type.
7. ודא שלחצן האפשרויות Dial-up To Private Network לחוץ, ולחץ Next.

   יופיע המסך Phone Number To Dial.
8. אם ביכולתך לחייג לשרת RRAS, הקלד את מספר הטלפון של קו הטלפון, אליו מחובר המודם בשרת RRAS זה. אם אינך יכול לחייג לשרת, הקלד מספר טלפון כלשהו בתיבה זו.
9. לחץ Next. יופיע המסך Connection Availability.
10. לחץ Next. יופיע המסך Internet Connection Sharing.
11. לחץ Next. יופיע המסך Completing The Network Connection Wizard ובו החיבור, כששם ברירת המחדל שלו הוא Dial-up Connection.
12. לחץ Finish. תיבת הדו-שיח Connect Dial-up Connection תופיע.
13. אם אינך יכול להתקשר לשרת RRAS, לחץ Cancel. תצלומי מסכים יוצגו בהליך האופציונלי הבא, כדי לאפשר לך לראות מה מופיע בשרת RRAS כאשר נוצרת התחברות. אם ביכולתך לחייג לשרת RRAS השלם את הצעדים הבאים.

14. בתיבת הטקסט User Name הקלד Bob_Train (שים לב, בין השם הפרטי ושם המשפחה יש קו תחתון) ולחץ על לחצן Dial. תיבת ההודעה Error Connecting to Dial-up Connection המופיעה, מודיעה כי לחשבון משתמש זה אין הרשאות מתאימות לחיוג פנימה. כזכור, לחשבון המשתמש Bob Train הוגדרה הרשאה מסוג Deny Access Remote Access.

15. בתיבת הטקסט User Name הקלד **Jane_Doe** (שים לב, בין השם הפרטי ושם המשפחה יש קו תחתון), בתיבה Password הקלד **student**, ולחץ על לחצן Dial. תיבת ההודעה Connecting Dial-up Connection תופיע ב-Server02 והחיבור ייבדק, יאומת ויירשם. ב-Server02 תופיע ההודעה Connection Complete.

16. סמן את תיבת הסימון Do not display this message again, ולחץ OK. החשבון Jane Doe התחבר בהצלחה לשרת RAS, מכיון שבמאפייני חשבון המשתמש מוגדרת ההגדרה Allow Access.

17. בחלון Network and Dial-up Connection לחץ לחיצה כפולה על הסמל Dial-up Connection. תיבת הדו-שיח Dial-up Connection Status תופיע.

18. לחץ על Disconnect.

19. לחץ לחיצה כפולה על הסמל Dial-up Connection.

20. בתיבת הטקסט User Name הקלד **John_Smith** (שים לב, בין השם הפרטי ושם המשפחה יש קו תחתון) ולחץ על לחצן Dial.

    תיבת ההודעה Error Connecting to Dial-up Connection המופיעה, מודיעה כי לחשבון משתמש זה אין הרשאות מתאימות לחיוג פנימה. כזכור, לחשבון המשתמש John Smith הוגדרה הרשאה מסוג Control Access through Remote Access Policy.

21. ב-Server01, שחזר את חלון תוסף התוכנה Routing and Remote Access.

22. בחלון Tree, לחץ על הצומת Remote Access Policies.

23. לחץ לחיצה כפולה על המדיניות Allow Access If Dial-in Permission Is Enabled, שבחלונית הפרטים. תיבת הדו-שיח Allow Access If Dial-in Permission Is Enabled Properties תופיע.

24. בחלק If A User Matches The Conditions, לחץ על לחצן האפשרויות Grant Remote Access Permission ולחץ OK.

25. חזור ל-Server02.

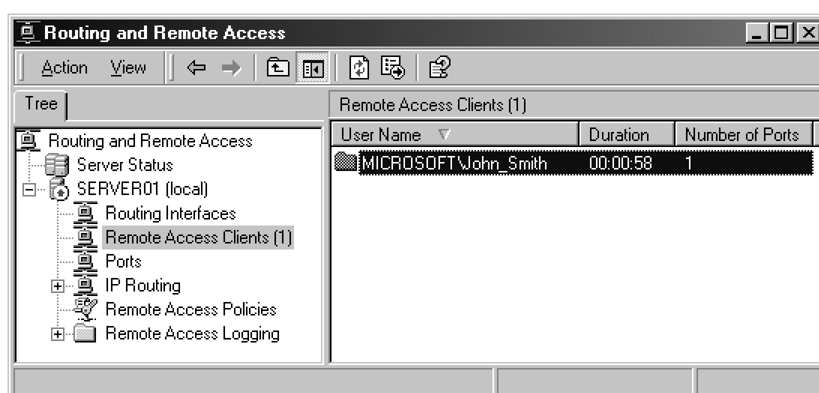
26. בתיבת הטקסט User Name לחץ על לחצן Dial ונסה שוב להתחבר בשם John_Smith. ב-Server02 תופיע תיבת ההודעה Connecting Dial-up Connection והחיבור ייבדק, יאומת ויירשם. מדיניות ברירת המחדל של גישה מרחוק מאפשרת כעת גישה לכל חשבונות המשתמשים, בהם נבחר לחצן האפשרויות Control Access through Remote Access Policy (בכרטיסיה Dial-in).

הליך 4: ניטור חיבור גישה מרחוק (אופציונלי)

אם יכולת להתחבר לשרת הגישה מרחוק, תוכל להשלים הליך זה. אם לא הצלחת להתחבר לשרת הגישה מרחוק, מוצגים בפניך בהליך זה תרשימי מסך חשובים. השלם הליך זה ב-Server01.

1. שחזר את תוסף התוכנה Routing and Remote Access.
2. בחלון Tree לחץ על Remote Access Clients (1).

בעמודה User Name יופיע MICROSOFT\John_Smith. שים לב שמופיעים גם משך החיבור ומספר היציאות המוקצות לחיבור זה (תרשים 10.12).



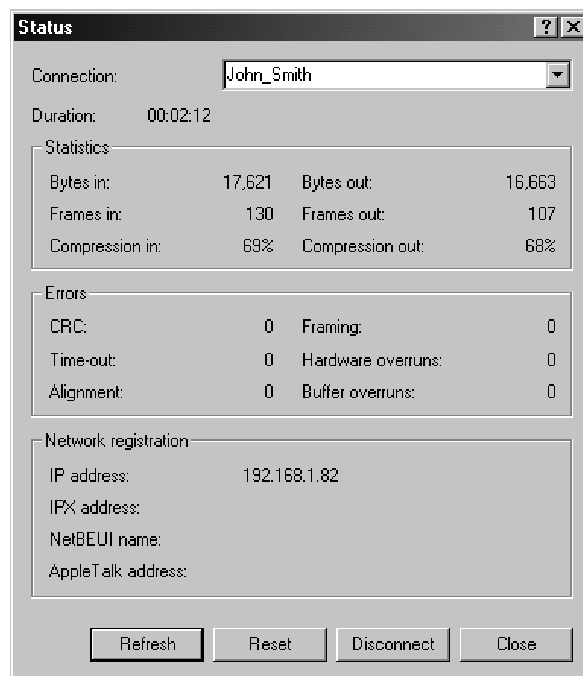
תרשים 10.12 שם המשתמש, משך החיבור ומספר היציאות המוקצות לו.

3. בחלונית הפרטים לחץ לחיצה כפולה על MICROSOFT\John_Smith.

תיבת הדו-שיח Status תופיע (ראה תרשים 10.13).

שים לב שהפרוטוקול היחיד הרשום לחיבור זה הוא TCP/IP. זאת מכיוון שכל הערכים שבחלק Network Registration ריקים, חוץ מאשר IP Address. כתובת ה-IP המוצגת, הוקצתה על ידי DHCP, מאחר שהגדרות ברירת המחדל של שרת RAS הן להיעזר ב-DHCP להקצאת כתובות IP ללקוחות גישה מרחוק. תוכל לוודא נתון זה בתוסף התוכנה DHCP ב-Server01.

בחלונית הפרטים תוכל גם לשלוח הודעה ללקוח הגישה מרחוק הנבחר, או לכל הלקוחות המחוברים, ולנתק לקוח גישה מרחוק.



תרשים 10.13 תיבת הדו-שיח Status של המשתמש מציגה נתוני TCP/IP.

4. סגור את תיבת הדו-שיח Status.
5. לחץ Start, ולחץ Run.
6. בתיבת הטקסט Open הקלד **c:\winnt\system32\logfiles\iaslog.log** ולחץ OK.

יומן ניהול החשבונות (Accounting Log) יוצג בפנקס הרשימות (Notepad). אם לא הצלחת להשלים תרגיל זה, פתח את הקובץ iaslog.log שבתקליטור המצורף לספר זה (בתיקיה Chapt10\ex2\). קובץ זה מכיל רק את שתי השורות האחרונות שנוצרו על ידי חשבון המשתמש John Smith.

למידע נוסף כיצד לקרוא ולפרש קובץ יומן זה, פתח את קובץ העזרה של IAS, וחפש בו אחר הערך IAS-Formatted Log Files. למבנה קריא יותר הכולל כמות קטנה יותר של נתונים מומלץ להגדיר את מבנה הקובץ (File Format) למבנה תואם מסד נתונים (Database-Compatible File Format).

7. סגור את Notepad.
8. כדי לצפות בתוצאות רישום אירוע ביומן, פתח את Event Viewer מקבוצת התוכניות Administrative Tools (בתפריט Start, Programs).

תוסף התוכנה Event Viewer יופיע ותוכן System Log יופיע בחלונית הפרטים.

9. אתר ולחץ לחיצה כפולה על אירוע יומן שמספר הזיהוי שלו (Event ID) 20015 ובשמו מופיע Source of RemoteAccess. אירוע חיבור בגישה מרחוק יופיע ויציג בפניך מי התחבר ולאיזו יציאה.

10. לחץ OK.

11. אתר ולחץ לחיצה כפולה על אירוע יומן שמספר הזיהוי שלו (Event ID) 20187 ובשמו מופיע Source of RemoteAccess.

אירוע חיבור בגישה מרחוק יופיע, ויציג בפניך שניסיון אימות גישה מרחוק נכשל ואת שם המשתמש, לגביו נכשל ניסיון ההתחברות.

12. לחץ OK, וסגור את תוסף התוכנה Event Viewer.

סיכום שיעור

גישה מרחוק של Windows 2000 מאפשרת שני סוגי התחברות בגישה מרחוק: גישה מרחוק בחיוג (Dial-up Remote Access) וגישה מרחוק ב-VPN (VPN Remote Access). חיבורי גישה מרחוק בחיוג כוללים לקוח גישה מרחוק, שרת גישה מרחוק ותשתית WAN. פרוטוקולים של גישה מרחוק שולטים ביצירת החיבור ובהעברת הנתונים דרך קישורי WAN. קיימים שלושה סוגים של פרוטוקולי גישה מרחוק, הנתמכים על ידי Windows 2000: PPP, SLIP ו-Asynchronous NetBEUI. גישה מרחוק של Windows 2000 תומכת בפרוטוקולי LAN הבאים: TCP/IP, IPX, AppleTalk ו-NetBEUI. לגישה מרחוק של Windows 2000 יש מיגוון מאפייני אבטחת מידע, כולל אימות מאובטח של משתמש, אימות הדדי, הצפנת נתונים, שיחה חוזרת, שיחה מזוהה ונעילת חשבון גישה מרחוק. ניהול גישה מרחוק כולל ניהול משתמשים, כתובות, גישה ואימות.

שיעור 4:
VPN - Virtual Private Networks

רשת פרטית וירטואלית (**V**irtual **P**rivate **N**etwork - VPN) היא הרחבה של הרשת הפרטית, הכוללת בחובה קישורים משולבים, מוצפנים ומאומתים באמצעות רשתות משותפות או ציבוריות. VPN מחקה את מאפייניה של רשת פרטים ייעודית ומאפשרת העברת נתונים בין שני מחשבים באמצעות רשת רחבת היקף, כגון האינטרנט. ניתן לדמות חיבורי נקודה-לנקודה תוך שימוש בתיעול (Tunneling), ואילו חיבורי LAN ניתן לדמות, תוך שימוש ברשתות LAN וירטואליות (VLANs). שיעור זה יציג בפניך את VPN ואת יסודות התיעול. הוא יסביר לך כיצד לנהל את שרת RAS שלך עבור VPN, וגם כיצד לאתר ולטפל בתקלות VPN פשוטות.

לאחר שיעור זה, תוכל

- לתאר את מאפייניה הבסיסיים של VPN ושל תיעול, כולל פרוטוקולי התיעול הנפוצים ביותר.
- לנהל שרתי VPN.
- לאתר ולטפל בתקלות VPN.

זמן לימוד משוער: 45 דקות

מבוא לרשתות וירטואליות פרטיות

רשתות וירטואליות פרטיות (**V**irtual **P**rivate **N**etworks - VPN) מאפשרות למשתמשים העובדים מביתם או הנעים בדרכים להתחבר באופן מאובטח לשרת ארגוני מרוחק, תוך שימוש בתשתית הניתוב, אותה מספקת רשת ציבורית רחבת היקף כגון האינטרנט. מנקודת מבטו של המשתמש, VPN היא חיבור מנקודה-לנקודה בין מחשב המשתמש והשרת בארגון. טיבה של הרשת רחבת ההיקף אינו רלוונטי, מכיון שנראה כאילו הנתונים נשלחים באמצעות קישור פרטי ייעודי.

טכנולוגיית VPN מאפשרת גם לארגון להתחבר לסניפיו, או לחברות אחרות, באמצעות רשת ציבורית רחבת היקף, ועדיין לשמור על תקשורת מאובטחת. חיבור VPN באמצעות האינטרנט מתפקד באופן לוגי כקישור WAN ייעודי.

החיבור המאובטח דרך הרשת רחבת ההיקף נראה למשתמש כממשק רשת וירטואלי, המספק תקשורת רשת פרטית ברשת ציבורית רחבת היקף. במקום שהמשתמש המרוחק יבצע שיחת חוץ יקרה (או שיחת חינם) לשרת ה- NAS (**N**etwork **A**ccess **S**erver) של הארגון, או לזה העומד לרשות הארגון, המשתמש מחייג לספק שירותי אינטרנט מקומי. תוך שימוש בחיבור לספק שירותי האינטרנט המקומי, נוצר חיבור VPN בין המשתמש בחיוג ושרת VPN של הארגון באמצעות האינטרנט.

הערה למידע נוסף אודות רישות פרטי וירטואלי, קרא את המסמך VPNoverview.doc שבתיקיה Chapt10\articles\ בתקליטור המצורף לספר זה.

חיבור רשתות באמצעות האינטראנט

בעת התחברות לרשתות באמצעות האינטרנט, יכולים סניפי החברה להשתמש בקווים ייעודיים (Dedicated Lines) או בקווי חיוג (Dial-up Lines).

קווים ייעודיים

במקום למשוך קווים ייעודיים ישירים ויקרים בין סניפי החברה והרכזת (Hub) הארגונית, מתחברים סניפי החברה ונתבי רכזות הארגון לאינטרנט, באמצעות תשתית קווי נל״ן קיימת וספק שירותי האינטרנט. תוך ניצול חיבורי ספק השירות המקומי, נוצר VPN בין נתב סניף החברה ונתב רכזת הארגון, באמצעות האינטרנט.

קווי חיוג

במקום שהנתב במשרדי סניף החברה יבצע חיוג לשיחות בינעירוניות או בינלאומיות לשרת גישה לרשת (NAS) של הארגון, או לשרת העומד לרשות הארגון – מתקשר הנתב לספק שירותי האינטרנט המקומי. מהחיבור לספק שירותי האינטרנט המקומי נוצר קשר VPN בין נתב הסניף לנתב רכזת הארגון, דרך האינטרנט. נתב רכזת הארגון, המשמש כשרת VPN, חייב להיות מחובר לספק שירותי האינטרנט המקומי שלו באמצעות קווים ייעודיים (קווי נל״ן). שרת VPN חייב להיות בהאזנה ובהמתנה לתנועת VPN במשך 24 שעות ביממה.

הערה בין אם הסניף משתמש בקווים ייעודיים ובין אם הוא משתמש בקווי חיוג רגילים, העברת הנתונים באמצעות VPN אינה תלויית מרחק, מפני שנעשה שימוש בקישורים פיסיים מקומיים בלבד.

חיבור מחשבים באמצעות האינטרנט

ברשתות ארגוניות רחבות היקף שונות, נתוניהן של מחלקות מסוימות רגישים עד כדי כך, שרשת ה-LAN של אותה מחלקה מנותקת לחלוטין מיתרת הרשת הארגונית. בעוד שמצב כגון זה מגן על נתוני המחלקה, הוא גם יוצר בעיית נגישות למידע עבור משתמשים, שאינם מחוברים פיסית לאותה רשת LAN נפרדת.

VPN מאפשרת לרשת ה-LAN של המחלקה להיות מחוברת באופן פיסי לרשת רחבת ההיקף של הארגון כולו, באמצעות שרת VPN נפרד. שים לב ששרת VPN כזה, אינו משמש כנתב בין רשת ה-LAN של המחלקה לרשת הארגונית. משתמשים ברשת הארגונית, שיש להם את הנתונים המתאימים (בהתאם למדיניות הארגון), יכולים ליצור קישור VPN עם שרת VPN ולקבל גישה לאותם משאבים חסויים של המחלקה. בנוסף לכך, כל התקשורת באמצעות VPN יכולה להיות מוצפנת, לצורך סודיות. למעשה, הרשת המחלקתית נסתרת מעיניהם של משתמשים שאין להם את הנתונים המתאימים.

Tunneling

תיעול (Tunneling), ידוע גם בשם Encapsulation, הוא שיטה לשימוש בתשתית רשת רחבת היקף (Internetwork) להעברת מטענים. המטען (Payload) יכול להיות המסגרות (או המנות) של פרוטוקול אחר. במקום לשלוח את המסגרת, כפי שהופקה על ידי הצומת המפיק, מצורפת למסגרת כותרת נוספת. הכותרת הנוספת מספקת נתוני ניתוב, כך שהמטען המצורף יכול לחצות את תווך הרשת רחבת ההיקף. אז, מנותבות מנות המטען בתעלה שבין שתי נקודות הקצה ברשת המעבר. לאחר שהמסגרות מגיעות ליעדן ברשת המעבר הן מוסרות מהכותרת הנוספת, ומועברות ליעדן הסופי.

תהליך זה כולו (הוספת מטען הכותרת והעברת המנות) נקרא **תיעול** (Tunneling). הנתיב הלוגי, דרכו נעות המנות בעלות המטען הנוסף (Encapsulated Packets) ברשת המעבר (Transit Internetwork) נקרא **תעלה** (Tunnel).

Tunnel Maintenance and Data Transfer

הפונקציונליות הקיבוצית של פרוטוקול שימור התעלה ופרוטוקול העברת נתונים בתעלה, ידועה בשם פרוטוקול תיעול (Tunneling Protocol). כדי ליצור את התעלה חייבים שרת התיעול ולקוח התיעול להשתמש בפרוטוקול תיעול זהה. דוגמאות לפרוטוקולי תיעול הן PPTP ו-L2TP, אשר בהם נדון בהרחבה בהמשך שיעור זה.

Tunnel Maintenance Protocol

פרוטוקול שימור התעלה (Tunnel Maintenance Protocol) משמש כמכניזם לניהול התעלה. עבור טכנולוגיות תיעול מסוימות, כגון PPTP או L2TP, דומה התעלה לדו-שיח (Session): שתי נקודות הקצה של התעלה חייבות להסכים לתיעול, ולהיות מודעות לקיומה של התעלה. אבל, שלא כמו בדו-שיח, תעלה אינה מבטיחה העברת נתונים אמינה. נתונים המועברים באמצעות תעלה, נשלחים בדרך כלל באמצעות פרוטוקול מבוסס צרור נתונים (Datagram-based Protocol), כגון UDP, כאשר נעשה שימוש ב-L2TP או TCP לניהול תעלה ופרוטוקול GRE מותאם (Modified **G**eneric **R**outing **E**ncapsulation) כאשר נעשה שימוש ב-PPTP.

יצירת התעלה

תעלה חייבת להיווצר לפני שמתבצעת העברת נתונים. את יצירת התעלה יוזם צד אחד שלה, לקוח התיעול. בקצה השני של התעלה מקבל שרת התיעול את בקשת ההתחברות.

כדי ליצור את התעלה, מבוצע תהליך התחברות הדומה להתחברות PPP. שרת התיעול מבקש מלקוח התיעול לאמת את עצמו. לאחר שהוא מאושר על ידי שרת התיעול, מתבצע חיבור התעלה וניתן להתחיל בהעברת נתונים בה.

הודעות יצירת התעלה נשלחות על ידי לקוח התיעול לכתובת הרשת רחבת ההיקף של שרת התיעול. נשתמש באינטרנט לשם הדוגמה: לקוח התיעול שולח הודעת יצירת תעלה מכתובת תואמת-InterNIC שלו לכתובת תואמת-InterNIC של שרת התיעול באינטרנט. אם לקוח התיעול משתמש בחיוג לאינטרנט (Internet Dial-up User), ייעזר לקוח התיעול בכתובת IP, כפי שהוקצתה לו על ידי ספק השירות, ככתובת המקור ובכתובת IP של שרת התיעול ככתובת היעד.

החזקת התעלה בחיים

בטכנולוגיות תיעול מסוימות, כגון PPTP ו- L2TP, מרגע שנוצרה התעלה היא חייבת להמשיך ולהתקיים. שני קצוות התעלה חייבים להיות ערים למצב הצד השני של התעלה, במקרה ומתרחשת תקלה בהתחברות. שימור תעלה (Tunnel Maintenance) מבוצע בדרך כלל באמצעות תהליך שמירה-בחיים (Keep-Alive), אשר מתשאל את הקצה השני של התעלה, כשלא נשלחים נתונים (וכך גורם לתעלה להמשיך להיות פעילה).

סגירת התעלה

טכנולוגיות תיעול אחדות מאפשרות לכל צד של התעלה לסגור אותה בחינניות, על ידי שליחת הודעות סגירה (Termination Messages) מצד לצד.

פרוטוקול העברת נתונים בתעלה

לאחר שנוצרה התעלה, ניתן לשלוח נתונים מתועלים. פרוטוקול העברת נתונים בתעלה (Tunnel Data Transfer Protocol) מאגד את הנתונים שאמורים להיות מועברים בתעלה. כשלקוח התיעול שולח מטען מתועל לשרת התיעול, הוא גם מצרף למטען כותרת של פרוטוקול העברת נתונים בתעלה. המטען שנוצר כתוצאה מאיגוד זה נשלח דרך רשת המעבר רחבת ההיקף ומנותב אל שרת התיעול.

שרת התיעול מקבל את המנות, מסיר את כותרת פרוטוקול העברת הנתונים בתעלה ומעביר את המטען ליעדו. מידע הנשלח בין לקוח ושרת התיעול מטופל באופן דומה.

סוגי תיעול

קיימים שני סוגים בסיסיים של תעלות: תעלה רצונית (Voluntary Tunnel) ותעלה כפויה (Compulsory Tunnel). בהתאם לתצורת הלקוח, תעלות כפויות עשויות להכיל תעלה כפויה קבועה או תעלה כפויה דינמית.

Voluntary Tunnels

תעלות רצוניות (Voluntary Tunnels) מוגדרות ונוצרות על ידי פעולה מודעת של המשתמש במחשב לקוח התיעול. מחשב המשתמש הוא נקודת קצה של תעלה ומתפקד כלקוח התיעול.

תיעול רצוני מתרחש, כאשר תחנת העבודה של הלקוח "מתנדבת" ליצור את התעלה אל שרת התיעול, שהוא היעד. מאחר שהלקוח מתפקד כלקוח תיעול, חייב להיות מותקן בו פרוטוקול התיעול המתאים. תיעול רצוני יכול להתרחש באחד המקרים הבאים:

- ❖ הלקוח כבר מקושר לרשת המעבר, שיכולה לספק ניתוב למטענים מאוגדים (Encapsulated Payloads) בין מחשב הלקוח לשרת התיעול הנבחר.
- ❖ ייתכן שעל הלקוח ליצור קשר (על ידי חיוג) עם רשת המעבר (Transit Internetwork) לפני שהלקוח יכול ליצור תעלה (זהו המקרה הנפוץ יותר). הדוגמה הטובה ביותר לאירוע מסוג זה היא משתמש אינטרנט בחיוג. משתמשי אינטרנט בחיוג צריכים לחייג למחשבי ספק שירותי האינטרנט, כדי ליצור קישור לאינטרנט, לפני שניתן יהיה ליצור תעלה דרך רשת האינטרנט.

Compulsory Tunnels

תעלה כפויה (Compulsory Tunnel) מוגדרת ונוצרת באופן אוטומטי עבור המשתמשים, מבלי שידעו על כך ומבלי שיצטרכו להיות מעורבים בתהליך. במקרה של תעלות כפויות, מחשב הלקוח אינו נקודת קצה של התעלה. התקן אחר בין מחשב הלקוח ושרת התיעול הוא נקודת הקצה של התעלה ומתפקד כלקוח תיעול (Tunnel Client).

אם במחשב הלקוח לא מותקן פרוטוקול התיעול, אך עדיין קיים הצורך ליצור תיעול, כי אז אפשר שמחשב אחר, או התקן רשת כלשהו ייצרו את התעלה בשמו של מחשב הלקוח. פעולה כגון זו נקראת **מרָכֵּז גישה** (Access Concentrator). כדי להפעיל את מרכז הגישה חייב שיהיה מותקן בו פרוטוקול התיעול המתאים וצריך שתהיה לו היכולת ליצור את התעלה כאשר מחשב הלקוח מבקש זאת.

כאשר מתחברים דרך האינטרנט, מתקשר מחשב הלקוח למחשב NAS, המאפשר תיעול אצל ספק שירותי האינטרנט. לדוגמה, ארגון יכול להסכים עם ספק שירותי אינטרנט על הקמת רשת מרָכְזי גישה בכל אתרי הגישה של הספק. מרָכזי גישה אלה יכולים ליצור תעלות דרך האינטרנט לשרת תיעול, המחובר לרשת הפרטית של הארגון. תצורה זו מוכרת בכינוי תיעול כפוי (Compulsory Tunneling), מכיון שהלקוח מחוייב

להשתמש בתעלה שנוצרה על ידי מרכז הגישה. לאחר שנוצר החיבור הראשוני, כל תנועת הרשת, אל הלקוח וממנו, נשלחת באופן אוטומטי דרך התעלה.

בתיעול כפוי, יוצר מחשב הלקוח חיבור PPP יחיד, וכאשר הוא מחייג אל NAS נוצרת תעלה וכל תנועת הנתונים מנותבת דרך תעלה זו.

הקביעה של מרכז הגישה לתעל לקוח חיוג לשרת תיעול מסוים, יכולה להיות מבוססת על נתונים קבועים המוגדרים במרכז הגישה, או על ידי דיון דינמי עם מסד נתוני הלקוח.

Static Compulsory Tunnels

תצורת תיעול קבוע (Static Compulsory Tunnels) דורשת בדרך כלל ציוד ייעודי (תיעול אוטומטי), או הגדרת תצורה ידנית (תיעול מבוסס-תחום, Realm-based Tunneling).

תיעול אוטומטי הוא מצב בו כל לקוחות החיוג למרכז הגישה מתועלים באופן אוטומטי לשרת תיעול מסוים. דבר זה דורש קווי גישה מקומיים ייעודיים וציוד גישה לרשת, ואת העלויות הנגזרות. לדוגמה, משתמשים עשויים להידרש להתקשר למספר טלפון מסוים, כדי להתחבר למרכז גישה אשר מצידו מתעל את כל החיבורים לשרת תיעול מסוים.

בשיטת Realm-based Tunneling בוחן מרכז הגישה חלק משם המשתמש (הנקרא Realm), כדי לקבוע לאן עליו לנתב את תנועת הנתונים המשויכת למשתמש זה. לדוגמה, משתמשים ב-domain בשם microsoft.com (הנכנסים לרשת בשם user@microsoft.com), יתועלו ליעד אחד, בעוד שמשתמשים מה-Domain בשם domain.com (הנכנסים לרשת בשם user@domain.com), יתועלו ליעד אחר. Realm-based Tunneling הוא די פשוט ליישום, אינו דורש ציוד ייעודי ויש לו תקורת מחיר נמוכה יחסית לאחר הגדרת התצורה הראשונית. אולם, שינויים בהגדרות או בתצורה עלולים להיות יקרים ולגזול זמן רב. בנוסף, כל התנועה של כל המשתמשים מאותו Realm מתועלת לאותו יעד. Realm-based Tunneling אינו מאפשר תיעול למספר יעדי שרתי תיעול.

Dynamic Compulsory Tunnels

בתיעול כפוי דינמי (Dynamic Compulsory Tunnels), הבחירה של יעד התיעול מתבצעת על בסיס משתמש, בעת שהוא מתחבר למרכז הגישה. משתמשים מאותו Realm יכולים להיות מתועלים ליעדים שונים, בהתאם לפרמטרים כגון, שם משתמש, מספר הטלפון ממנו הוא מחייג, מחלקה, מיקום ואפילו השעה ביום. תעלות דינמיות מאפשרות את הגמישות הרבה ביותר מכל שיטת תיעול כפייתי אחרת.

תיעול דינמי גם מאפשר למרכז הגישה להיות NAS מרובה שימושים, דהיינו לאפשר חיבורים של לקוחות מתועלים ולקוחות אינטרנט רגילים (שאינם מתועלים). לא נדרש מרכז גישה ייעודי או קו טלפון ייעודי. כדי שמרכז הגישה ידע האם יש לתעל את הלקוח המתחבר אליו או לא, עליו להיוועץ במסד נתונים.

בעוד שכל מרכז גישה יכול לאחסן את מסד הנתונים שלו של נתוני משתמשים, זהו איננו פתרון טוב, מבחינה מנהלתית. פתרון טוב יותר הוא לאחסן את נתוני המשתמשים במיקום מרכזי אחד, ולדאוג שמרכז הגישה יבדוק את מסד הנתונים המרכזי, כאשר הוא נדרש (כשלקוח בחיוג מתקשר). פתרון אפשרי לנושא ריכוזיות מסד הנתונים ניתן למצוא בשרת RADIUS.

פרוטוקולים VPN

הפרוטוקולים העיקריים בהן משתמשת Windows 2000 לצורך גישת VPN הם PPTP, L2TP, IPSec ו-IP-IP. פרוטוקולים אלה יכולים לעבוד יחדיו, או כל אחד לחוד.

PPTP

PPTP (**P**oint-to-**P**oint **T**unneling **P**rotocol, פרוטוקול תיעול מנקודה לנקודה) הוא הרחבה של PPP. הפרוטוקול מאגד מסגרות PPP לצרורות נתוני IP, לשם העברתן ברשת IP רחבת היקף כגון האינטרנט. PPTP יכול גם לשמש ברישות LAN-to-LAN פרטי.

PPTP משתמש בחיבור TCP לשימור התעלה, ובמסגרות PPP, המאוגדות בפרוטוקול GRE מותאם (Modified GRE), לתיעול נתונים. המטען של מסגרות PPP המאוגדות יכול להיות מוצפן ודחוס.

PPTP נוצר על ידי פורום PPTP, הכולל את חברת Microsoft, Ascend Communications, 3COM, ECI Telematics ו- US Robotics.

תעלות PPTP חייבות להיות מאומתות באמצעות אותו מכניזם אימות של PPP (PAP, MS-CHAP, CHAP או EAP). PPTP יורש את ההצפנה ואת הדחיסה של מטען PPP מ-PPP. ב-Windows 2000, ניתן להשתמש בדחיסת PPP רק כאשר פרוטוקול האימות הוא EAP-TLS או MSCHAP. הצפנת PPP מספקת סודיות בין נקודות הקצה של התעלה בלבד. אם נדרשת אבטחה ברמה גבוהה יותר או אבטחת נתונים מקצה לקצה, ניתן להשתמש ב-IPSec. תרשים 10.14 מציג את מבנה מנת PPTP.

Data-link Header	IP Header	GRE Header	PPP Header	Encrypted PPP Payload (IP Datagram, IPX Datagram, NetBEUI Frame)	Data-link Trailer

תרשים 10.14 מנת PPTP מציגה את הנתונים המוצפנים הנשלחים, כולל נתוני כותרת (Header) **ושובל** (Trailer).

L2TP

L2TP (**L**ayer **2** **T**unneling **P**rotocol) הוא שילוב של PPTP ושל L2F (**L**ayer **2** **F**orwarding). זוהי טכנולוגיה שהוצעה על ידי חברת Cisco. L2PT הוא עירוב של המאפיינים הטובים של PPTP ושל L2F.

L2PT הוא פרוטוקול רשת, המאגד מסגרות PPP לשליחה דרך IP, X.25, ממסר מסגרת (Frame Relay) או ATM. כאשר מנצלים את IP לצורך הנעת צרורות הנתונים, יכול L2TP לשמש כפרוטוקול תיעול באינטרנט. L2TP יכול גם לשמש ברישות LAN-to-LAN פרטי.

הערה L2TP בסביבת Windows 2000 **יכול לפעול** רק ברשת IP. **הוא אינו פועל** ברשת Windows 2000 טהורה (Native Mode), דרך X.25, ממסר מסגרת (Frame Relay) **או** ATM.

L2TP משתמש ב-UDP וברצף הודעות L2TP לשימור התעלה. L2TP גם משתמש ב-UDP כדי לשלוח מסגרות PPP מאוגדות באמצעות L2TP כנתונים המתועלים. המטען של מסגרות PPP מאוגדות יכול להיות מוצפן ודחוס. Microsoft אמנם בחרה בהצפנת IPSec עבור L2TP, במקום הצפנת PPP, אולם יישומים אחרים של L2TP יכולים להשתמש בהצפנת PPP. תרשים 10.15 מציג מנת L2TP, המוכנה לשליחה באמצעות הגדרות אימות והצפנה של IPSec, דרך חיבור WAN נקודה-לנקודה, כגון קו חיוג. בתרשים מתוארים גם צעדי עיבוד המנה. צעדים 1-4 מציגים עיבוד רגיל הקודם לאיגוד IPSec. צעדים 5-7 מציגים את תהליך IPSec. יתר הצעדים נדרשים כדי לשלוח את המנה ברשת ליעדה הסופי.

Data-link Header	IP Header	IPSec ESP Header	UDP Header	L2TP Header	PPP Header	PPP Payload (IP Datagram, IPX Datagram, NetBEUI Frame)	IPSec ESP Trailer	IPSec ESP Auth Trailer	Data-link Trailer

תרשים 10.15 מנת L2TP מציגה נתונים מוצפנים באמצעות **אימות** IPSec, **כותרת** IP נוספת ונתוני כותרת ושובל לקישור נתונים (Data-Link).

במהותו דומה L2TP מאוד ל-PPTP. תעלת L2TP נוצרת בין לקוח L2TP ושרת L2TP. הלקוח יכול להיות מחובר כבר לרשת IP רחבת היקף (כגון LAN) אשר יכולה להגיע את שרת התיעול, או שלקוח יכול להידרש לחייג אל NAS, כדי להקים חיבוריות IP (במקרה של משתמשי אינטרנט בחיוג).

יצירת תעלות L2TP חייבת להיות מאומתת, תוך שימוש באותו מכניזם אימות, כפי שהדבר בחיבורי PPP (PAP, CHAP, MS-CHAP או EAP). L2TP יורש את דחיסת PPP, אך לא את ההצפנה שלו. לא נעשה שימוש בהצפנת PPP, מפני שהיא אינה עונה על דרישות אבטחת המידע של L2TP. הצפנת PPP מסוגלת לספק סודיות, אך אינה מספקת הגנה לאימות, שלמות ושידור חוזר של כל מנה ומנה. הצפנת הנתונים נעשית על ידי IPSec. השימוש בהצפנת חיבור של PPP עם הצפנת המטען של IPSec מגדיל את תקורת העיבוד ויש לו תועלת מעטה, אם בכלל.

PPTP לעומת L2TP

גם PPTP וגם L2TP משתמשים ב-PPP לצורך חיבוריות WAN נקודה-לנקודה, כדי לספק מעטפת ראשונית לנתונים ואחר כך להוסיף כותרות לשם העברה באמצעות רשת מעבר. אולם, קיימים הבדלים מסוימים בין PPTP לבין L2TP:

- PPTP דורש שרשת המעבר תהיה רשת IP. L2TP דורש רק שתיווך התעלה (Tunnel Media) יספק חיבוריות נקודה-לנקודה מוכוונת-מנות (Packet Oriented Point-to-Point Connectivity). L2TP יכול לעבור ב-IP (תוך שימוש ב-UDP), מעגלי ממסור מסגרות וירטואליים קבועים (Frame Relay PVCs), מעגלי X.25 וירטואליים (X.25 VCs) או מעגלי ATM וירטואליים (ATM VCs).
- L2TP מספק אפשרויות דחיסת כותרות. כאשר דחיסת כותרות זמינה, פועל L2TP בתקורה של 4 בתים, בהשוואה לתקורה של ששה בתים ב-PPTP.
- L2TP מספק גם אימות תעלה, בעוד ש-PPTP אינו עושה זאת. אולם כאשר PPTP או L2TP פועלים על IPSec, הוא עצמו מספק את אימות התיעול - מה שהופך את אימות התיעול של שכבה 2 (Layer 2 Tunnel Authentication) לבלתי דרוש.
- PPTP משתמש בהצפנת PPP, בעוד ש-L2TP אינו עושה זאת. L2TP של Microsoft דורש IPSec לצורך ההצפנה.

IPSec

IPSec, פרוטוקול תיעול בשכבה 3, הוא קבוצת תקנים התומכת בהעברה מאובטחת של נתונים דרך רשת IP רחבת היקף.

מצב IPSec Encapsulating Security Payload (ESP) Tunnel תומך באיגוד והצפנה של צרור נתונים שלם לצורך העברה מאובטחת דרך רשת IP פרטית או ציבורית.

במצב IPSec ESP Tunnel מאוגד ומוצפן צרור נתוני IP שלם עם ESP. התוצאה מאוגדת אז, תוך שימוש בכותרת טקסט רגיל של IP (Plaintext IP Header), ונשלחת לרשת המעבר (ראה תרשים 10.15).

עם קבלת צרור הנתונים המוצפן, שרת התיעול מעבד ומסיר את כותרת הטקסט הפשוט של IP ומאמת ומפענח את ESP ואת מנת ה-IP. אז מעובדת מנת ה-IP באופן רגיל. עיבוד רגיל יכול לכלול שליחת המנה ליעדה הסופי.

ESP Tunnel Mode vs. Transport Mode

ההבדל העיקרי בין מצב תעלה מול מצב העברה של ESP הוא, שלראשון יש כותרת UP מאוגדת. בשל כותרת זו, כאשר המנה יוצאת מהתעלה (כאשר מוסרים האיגוד וההצפנה של IPSec), היא יכולה להיות מנותבת ליעדה הסופי. בעת השימוש במצב העברה של ESP המנה מפוענחת תמיד כשהיא מגיעה ליעדה הסופי.

IPSec ESP Tunnel Mode Packet Structure

מצב תעלה של ESP ב- IPSec (IPSec ESP Tunnel Mode) מבוצע דרך מספר שכבות איגוד. תרשים 10.15 מתייחס לצעדים הבאים:

- **שכבת איגוד ראשונה** (First Layer of Encapsulation) – לצרור נתוני IP הראשוני מצורף שובל ESP, ואז הוא מוצפן (צעד 5 בתרשים).
- **שכבת איגוד שנייה** (Second Layer of Encapsulation) – המטען המוצפן מאוגד עם כותרת ESP ושובל אימות שלESP . שובל האימות של ESP מכיל את ערך בדיקת השלמות (**I**ntegrity **C**heck **V**alue - ICV) - סכום בדיקת קריפטוגרפיה, המשמש לאימות ובדיקת שלמות המטען (צעדים 6 ו-7).
- **שכבת איגוד שלישית** (Third Layer of Encapsulation) – מנת IPSec מאוגדת עם כותרת IP סופית, המכילה את כתובות ה-IP של המקור והיעד של נקודות הקצה של התעלה (צעד 8).
- **שכבת איגוד קישור הנתונים** (Data Link Layer of Encapsulation) – כדי להישלח בקישור WAN או LAN, מאוגד לבסוף צרור הנתונים עם כותרת ושובל עבור טכנולוגיית קישור הנתונים של ממשק היציאה הפיסי (צעדים 9 ו-10).

מצב תעלה של IPSec הוא טכניקת תיעול של שכבה 3 במודל OSI (שכבת הרשת). שלא כמו PPTP ו-L2TP, מצב תעלה של IPSec אינו סומך על PPP לאימות או הצפנה. בנוסף, הוא אינו יכול לשמש כממשק נתב Windows 2000, כפי שיכול IP-IP. מכיון שמצב תעלה של IPSec אינו יכול להוות ממשק נתב, הוא אינו יכול לתמוך בפרוטוקולי ניתוב או בחיוג-על-פי-דרישה (Dial on Demand). במקום זאת, מצב תעלה של IPSec יכול לשמש בהתבסס על מסנני מנות (Packet Filters) בכל נתיב. מסנני המנות קובעים את יעד תעלת IPSec.

IP-IP

IP-IP, או IP בתוך IP, הוא טכניקת תיעול פשוטה בשכבה 3 של מודל OSI (שכבת הרשת). רשת וירטואלית נוצרת על ידי איגוד מנת IP עם כותרת IP נוספת. השימוש העיקרי ב- IP-IP הוא לשם תיעול תעבורת שידור לרבים (Multicast) בחלקים של הרשת, שאינם תומכים בניתוב שידור לרבים (Multicast Routing). מבנה מנת IP-IP כולל את כותרת IP החיצונית, כותרת התעלה, כותרת IP הפנימית ואת מטען ה-IP.

מטען ה-IP כולל את כל מה שמעל IP. זה יכול להיות כותרות TCP, UDP או ICMP, ונתונים. צורה מינימלית של שימור התעלה מתאפשרת באמצעות הודעות ICMP פשוטות. הודעות ICMP מאפשרות לתעלה לבצע גילוי MTU של תעלה, ולזהות עומסים ותקלות ניתוב.

ניהול רשתות וירטואליות פרטיות

בשיעור 3 למדת כיצד לנהל גישה מרחוק. באופנים רבים דומה ניהול רשתות פרטיות וירטואליות לניהול גישה מרחוק. רישות פרטי וירטואלי חייב להיות מנוהל בדיוק כמו כל משאב רשת אחר, ונושא אבטחת המידע ב-VPN חייב להיות מנוהל בקפידה, ובמיוחד כשמדובר בחיבורי VPN דרך האינטרנט.

ניהול משתמשים

מאחר שאין זה פרקטי ליצור חשבונות משתמש שונים עבור אותו משתמש בשרתים שונים, רוב מנהלי המערכות מגדירים מסד נתונים ראשי לחשבונות ב-Domain Controller או בשרת RADIUS. דבר זה מאפשר לשרת VPN לשלוח את נתוני המשתמש לאימות, להתקן אימות מרכזי. אותו חשבון משתמש, משמש גם לגישה מרחוק בחיוג וגם לגישה מרחוק באמצעות VPN.

ניהול כתובות ושרתי שמות

לשרת VPN חייבות להיות כתובות IP זמינות, כדי שיוכל להקצות אותן לממשק הווירטואלי של שרת VPN וללקוחות VPN, בעת חלק המשא ומתן של IPCP (**IP C**ontrol **P**rotocol) של תהליך ההתחברות. כתובת IP המוקצית ללקוח VPN, מוקצית לממשק הווירטואלי של לקוח VPN.

עבור שרתי VPN מבוססי Windows 2000, כתובות ה-IP המוקצות ללקוחות VPN מתקבלות באמצעות DHCP, כברירת מחדל. ניתן גם להגדיר מקבץ כתובות IP קבועות. שרת VPN חייב גם להיות מוגדר עם שרתי הסדרת שמות (Name Resolution Servers). בדרך כלל יהיו כתובות אלו כתובות של שרתי DNS או שרתי WINS, כך שניתן יהיה להקצות אותן ללקוח VPN בעת משא ומתן IPCP.

ניהול גישה

ב-Windows 2000, הגדר את מאפייני החיוג פנימה (Dial-in Properties) בחשבונות המשתמש ובמדיניות הגישה מרחוק, כך שינהלו את הגישה עבור חיבורי רישות בחיוג ו-VPN.

גישה על פי חשבון משתמש

אם אתה מנהל גישה מרחוק על בסיס משתמש, לחץ על לחצן האפשרויות Allow Access בכרטיסיה Dial-in, שבתיבת הדו-שיח Properties של אותם חשבונות משתמשים, להם מותר ליצור חיבורי VPN. אם שרת VPN מאפשר רק חיבורי VPN, מחק את מדיניות ברירת המחדל לגישה מרחוק - Allow Access If Dial-In Permission Is Enabled. אחר כך, צור מדיניות גישה מרחוק חדשה בעלת שם תיאורי, כגון VPN Access If Allowed By User Account.

אזהרה לאחר מחיקת המדיניות, תידחה גישתו של לקוח חיוג אשר אינו תואם לפחות לאחת מהגדרות המדיניות שיצרת.

אם שרת VPN מאפשר גם שירותי גישה מרחוק בחיוג, אל תמחק את מדיניות ברירת המחדל, אלא העבר אותה, כך שהיא תהיה המדיניות האחרונה הנסקרת.

גישה על פי חברות בקבוצה

אם אתה מנהל את הגישה מרחוק על בסיס קבוצות, לחץ על לחצן האפשרויות Control Access through Remote Access Policy בכל חשבונות המשתמשים. צור קבוצת משתמשים של Windows 2000, בה יהיו חברים אותם משתמשים שלהם מותר לבצע גישה באמצעות VPN. אם שרת VPN מאפשר רק חיבורי VPN, מחק את מדיניות ברירת המחדל לגישה מרחוק - Allow Access If Dial-In Permission Is Enabled. אחר כך, צור מדיניות גישה מרחוק חדשה בעלת שם תיאורי, כגון VPN Access If Member Of VPN-Allowed Group, ואז החל את המדיניות על אותה קבוצת Windows 2000.

אם שרת VPN מאפשר גם שירותי גישה מרחוק בחיוג, אל תמחק את מדיניות ברירת המחדל, אלא העבר אותה, כך שהיא תהיה המדיניות האחרונה הנסקרת.

ניהול אימות

שרת VPN יכול להיות מוגדר להשתמש באימות RADIUS או באימות Windows. אם Windows נבחרה כספק האימות, מועברים נתוני משתמשים המנסים להתחבר לשרת VPN, למכניזם האימות של Windows, ומדיניות גישה מרחוק מוגדרת באמצעות תוסף התוכנה Routing and Remote Access.

אם נבחר RADIUS ומוגדר כספק האימות בשרת VPN, נשלחים נתוני המשתמש והפרמטרים של בקשת ההתחברות, כרצף הודעות בקשה של RADIUS לשרת RADIUS.

שרת RADIUS מקבל בקשה להתחברות של לקוח משרת VPN, ומאמת את המשתמש באמצעות מסד נתוני האימות שלו. שרת RADIUS יכול גם להחזיק מסד נתונים מרכזי ובו מאפיינים רלוונטיים נוספים אודות המשתמש. בנוסף לתגובת "כן" או "לא" לבקשת האימות, RADIUS יכול גם להודיע לשרת VPN אודות פרופיל התחברות המתאים למשתמש, כגון משך זמן מירבי להתחברות, הקצאת כתובת IP קבועה וכדומה. שרת IAS RADIUS מאחסן נתוני פרופיל גישה מרחוק עבור לקוחות המשתמשים בשרת RADIUS כספק האימות. אם מוגדר לשרת RAS אימות RADIUS, נעלם הצומת Remote Access Policies מחלון Tree של תוסף התוכנה Routing and Remote Access, ואז גם מוגדרת מדיניות גישה מרחוק ב-IAS.

RADIUS יכול להגיב לבקשות אימות בהתבסס על מסד הנתונים שלו, או שהוא יכול להוות חזית לשרת מסד נתונים אחר, כגון שרת ODBC גנרי או Windows 2000 Domain Controller. האחרון יכול להיות ממוקם באותו מחשב בו מוגדר שרת RADIUS, או במקום אחר. בנוסף, שרת RADIUS יכול לתפקד כלקוח Proxy לשרת RADIUS מרוחק.

איתור תקלות

איתור תקלות ב-VPN דורש שילוב של איתור תקלות בחיבוריות IP, ביצירת חיבוריות גישה מרחוק, בניתוב וב-IPSec. דרושה הבנה טובה בכל הנושאים הללו.

החלקים הבאים מציגים תקלות VPN שכיחות ואת כלי האיתור והטיפול בהן, המסופקים עם Windows 2000. תקלות VPN ייכנסו בדרך כלל לקטגוריות הבאות:

- ניסיון התחברות נדחה, למרות שהיה אמור להתקבל.
- ניסיון התחברות התקבל, למרות שהיה אמור להידחות.
- לא ניתן להגיע לאתרים מעבר לשרת VPN.
- לא מסוגל ליצור תעלה.

ניסיון התחברות נדחה, למרות שהיה אמור להתקבל

ודא כי הנקודות הבאות תקינות כדי לאתר ולטפל בתקלה זו:

- באמצעות הפקודה ping, ודא כי ניתן לגשת אל שם המארח (Host Name) או לכתובת ה-IP של שרת VPN. אם נעשה שימוש בשם מארח, ודא כי הוא מומר נכון לכתובת ה-IP שלו.
- ודא כי בשרת VPN פועל RRAS.
- ודא שלא כל יציאות PPTP או L2TP בשרת VPN בשימוש, וכי יש יציאות פנויות. אם יש צורך בכך, שנה את מספר יציאות PPTP ל-L2TP, כדי לאפשר יותר חיבורים בו-זמנית. יציאות מוספות ומוגדרות מהצומת Ports שבתוסף התוכנה Routing and Remote Access.
- ודא כי פרוטוקול התיעול בלקוח VPN נתמך על ידי שרת VPN. תוכל לעשות זאת על ידי בחינת Port Properties בשרת RAS.
- לקוחות גישה מרחוק ל-VPN מוגדרים כברירת מחדל לסוג שרת Automatic. משמעות הדבר היא שהם ינסו ליצור תיעול PPTP קודם כל, ואחר כך ינסו ליצור תיעול L2TP על IPSec. אם סוג השרת מוגדר כ-PPTP או כ-L2TP, ודא שפרוטוקול התיעול נתמך על ידי שרת ה-VPN.
- מחשב Windows 2000 המפעיל את RRAS הוא שרת PPTP ו-L2TP עם חמש יציאות L2TP וחמש יציאות PPTP, כברירת מחדל (מופיע בחלונית הפרטים של הצומת Ports בתוסף התוכנה Routing and Remote Access). כדי ליצור שרת המפעיל יציאות PPTP בלבד, קבע את מספר יציאות L2TP לערך 0 (אפס).

  כדי ליצור שרת המפעיל יציאות L2TP בלבד, קבע את מספר יציאות PPTP לערך 1, מפני שלא ניתן לקבוע אותו כאפס, ואז בטל את הסימון בתיבת הסימון Remote Access Connection (Inbound Only) ובתיבת הסימון Demand Dial Routing Connection (Inbound Only). את ההגדרות הללו יש לבצע מתיבת הדו-שיח של מאפייני הצומת Ports. במחשב הלקוח שנה את סוג שרת VPN מ- Automatic ל-L2TP (**L**ayer **2** **T**unneling **P**rotocol).
- ודא כי בשרת VPN ובלקוח VPN ניתן להפעיל לפחות שיטת אימות שכיחה אחת.
- לחיבורי PPTP - בדוק האם ניתן לבצע התחברות PPTP ללא הצפנה. אם כן, בדוק את הגדרות ההצפנה בלקוח ובשרת VPN.

- לחיבורי L2TP על IPSec - בדוק האם ניתן לבצע חיבור L2TP ללא הצפנה (ללא IPSec). אם כן, בדוק את הגדרות הצפנת L2TP על IPSec בלקוח ובשרת VPN.

  כדי לבטל את IPSec במחשב לקוח, פתח את מאפייני חיבור VPN. בחר בכרטיסיה Networking, ואז גש למאפייני Internet Protocol (TCP/IP). לחץ על Advanced, ובחר בכרטיסיה Options. לסיום, עבור למאפייני האפשרות IP Security. מתיבת הדו-שיח IP Security תוכל להגדיר את הלקוח, כך שלא יעשה שימוש ב- IPSec.

  כדי לבטל את IPSec בשרת, גש למאפייני מתאם הרשת המקומי. מכאן, גש למאפייני Internet Protocol (TCP/IP) ועקוב אחר התהליך שתואר לגבי מחשב הלקוח. ניתן לבצע תהליך זהה גם במחשב לקוח, אם בחלון Network and Dial-up Connections של מחשב הלקוח מופיע הסמל Local Area Connection.

- ודא כי לפרמטרים של ההתחברות יש הרשאות במדיניות הגישה מרחוק. מדיניות גישה מרחוק מוגדרת מתוך תוסף התוכנה Routing and Remote Access, או בשרת RADIUS, תלוי בספק האימות.

כדי שניתן יהיה ליצור את החיבור, חייבים הפרמטרים של החיבור לעמוד בתנאים הבאים:

- לעמוד בכל התנאים של מדיניות גישה מרחוק אחת לפחות.
- לקבל הרשאות גישה מרחוק, בין אם מאובייקט המשתמש (הגדרת Allow Access), ובין אם משילוב של הגדרות אובייקט המשתמש ושל מדיניות גישה מרחוק. במקרה האחרון, נבחרת האפשרות Control Access Through Remote Access Policy שבמאפייני User Object, ובמאפייני מדיניות הגישה מרחוק נבחרת האפשרות Grant Remote Access Permission.
- לתאום לכל הגדרות הפרופיל.
- לתאום לכל הגדרות החיוג פנימה (Dial-in) של אובייקט המשתמש. ודא כי הגדרות פרופיל מדיניות הגישה מרחוק, אינן מתנגשות עם מאפייני שרת הניתוב והגישה מרחוק.

אם הגדרות פרופיל מדיניות הגישה מרחוק התואמת, מתנגשות עם הגדרות שרת VPN, יידחה ניסיון ההתחברות. לדוגמה, אם הגדרת מדיניות הגישה מרחוק התואמת, מגדירה כי חובה להשתמש בפרוטוקול האימות EAP-TLS, ואילו EAP-TLS אינו פעיל בשרת VPN, שרת VPN ידחה את ניסיון ההתחברות.

- ודא כי נתוני המשתמש של לקוח VPN כוללים שם משתמש, סיסמה ושם Domain, וכי ניתן לאמת אותם בשרת VPN.
- אם בשרת VPN מוגדר מאגר כתובות IP קבועות, ודא שקיימות במאגר זה מספיק כתובות. אם כל הכתובות במאגר הכתובות הקבועות הוקצו ללקוחות VPN מחוברים, שרת VPN אינו יכול להקצות כתובות נוספות ולכן יידחה ניסיון ההתחברות.

- ודא את הגדרת ספק האימות. עבור שרת VPN, שהוא שרת-חבר (Member Server) ב-Windows 2000 Native or Mixed Mode Domain, אשר מוגדר לאימות Windows NT, ודא כי חשבון המחשב של מחשב שרת VPN הוא חבר בקבוצת האבטחה RAS and IAS Servers.

- לחיבורי גישה מרחוק ל-VPN - ודא כי אפשרות הגישה מרחוק פעילה בשרת VPN.

- לחיבורי גישה מרחוק ל-VPN - ודא כי היציאות PPTP ו/או L2TP זמינות לקבלת בקשות להתחברות בגישה מרחוק.

- ללקוחות מרוחקים של VPN - ודא שפרוטוקולי LAN, בהם משתמש הלקוח אכן זמינים לגישה מרחוק.

- לחיבורי VPN נתב-לנתב (Router-to-Router), ודא שהניתוב פעיל בשרת VPN, וכי נבחרו אפשרויות ניתוב חיוג-על-פי-דרישה וניתוב LAN. אפשרות זו ניתנת להגדרה ממאפייני צומת Ports.

ניסיון התחברות התקבל למרות שהיה אמור להידחות

ודא כי לא ניתנו הרשאות לפרמטרים של ההתחברות, מתוך מדיניות הגישה מרחוק.

כדי שהחיבור יידחה, חייבים הפרמטרים של ההתחברות להיות מוגדרים לדחיית חיבור גישה מרחוק, באמצעות אחת מהשיטות הבאות:

- הרשאת הגישה מרחוק באובייקט המשתמש מוגדרת Deny Access.

- הרשאת הגישה מרחוק באובייקט המשתמש מוגדרת Control Access through Remote Access Policy, ומדיניות הגישה מרחוק הראשונה התואמת את ניסיון ההתחברות מוגדרת Deny Remote Access Permission.

לא ניתן להגיע לאתרים מעבר לשרת VPN

ודא את הנתונים הבאים, כדי לאתר תקלה כגון זו:

- ללקוחות VPN מרוחקים, ודא כי האפשרות Entire Network נבחרה בפרוטוקולי LAN, בהם משתמשים לקוחות VPN.
- בחן את מאגר כתובות ה- IP שבשרת VPN.

- אם שרת VPN מוגדר לעבוד עם מאגר כתובות IP קבועות, בדוק שנתיב לטווח הכתובות המוגדרות על ידי מאגר הכתובות הקבועות, זמין למארחים ולנתבים באינטראנט. אם לא, יש להוסיף לנתבי האינטראנט נתיב IP, הכולל את מאגר כתובות ה-IP הקבועות של שרת VPN (כתובת IP ומסכת רשת משנה). נתיב לרשת ניתן ליישם באמצעות רשומות ניתוב סטטיות, או באמצעות פרוטוקול ניתוב, כגון RIP או OSPF.
- אם שרת VPN מוגדר לעבוד עם שרת DHCP לצורך הקצאת כתובות IP, ואין שרת DHCP זמין, צריך להוסיף לנתבי הרשת את הנתיב 169.254.0.0/16 (מסכת רשת משנה 255.255.0.0). כאשר שרת VPN מוגדר לעבוד עם שרת DHCP ואין שרת DHCP זמין, מקצה שרת VPN כתובות ממאגר הכתובות AutoNet, 169.254.0.0/16. כדי לבחון את הקצאת הכתובת במחשב לקוח, עבור למאפייני החיבור הפעיל.
- אם מאגר כתובת הIP הקבועות הוא טווח כתובות IP, שהוא תת קבוצה של טווח כתובות ה-IP של הרשת אליה מחובר שרת VPN, ודא כי טווח הכתובות במאגר כתובות ה-IP הקבועות אינו מוקצה לצמתי TCP/IP אחרים, בין אם באופן קבוע ובין אם באמצעות DHCP.
- ל-VPN נתב-לנתב - ודא כי חיבור VPN נתב-לנתב מתורגם על ידי שרת VPN כחיבור VPN נתב-לנתב, ולא כחיבור גישה מרחוק.
- אם שם המשתמש המופיע בנתוני הנתב מופיע ב- Dial-in Clients של Routing and Remote Access Manager, זאת אומרת ששרת VPN זיהה את הנתב המתקשר כלקוח גישה מרחוק. ודא כי שם המשתמש המופיע בנתוני הנתב, תואם לשם של ממשק חיוג-על-פי-דרישה בשרת VPN.

לא מסוגל להקים תיעול

ודא את הנתונים הבאים, כדי לאתר תקלה כגון זו:

❖ ודא כי אתה מתחבר לכתובת הנכונה. נסה להשתמש בכתובת ה-IP של ממשק השרת הקרוב אליך ביותר. זוהי כתובת הממשק, לה הנתיב חזרה אליך. אם אתה נעזר ב-DNS לצורך הסדרת כתובת IP, הכתובת הנכונה אינה אמורה להיות בשימוש. השימוש בכתובת שגויה יגרום לשיח PPTP להתאפס.

❖ ודא כי סינון המנות בממשק הנתב בין לקוח VPN ושרת VPN, אינו מונע את ההעברה של תנועת שימור התעלה או של הנתונים המתועלים.

- בשרת VPN של Windows 2000, ניתן להגדיר סינון מנות IP מההגדרות המתקדמות של TCP/IP ומתוך תוסף התוכנה Routing and Remote Access. חפש בשני המקומות מסננים אשר יכולים למנוע תנועת VPN.
- ודא כי סינון מנות בנתבים אחרים בנתיב, אינו חוסם את הפרוטוקולים הנדרשים.
- בחן את הגדרות תצורת פרוטוקולי התיעול:

♦ **PPTP** – מעביר TCP ביציאה 1723 וזיהוי 47 של פרוטוקול IP, לבקרת השיח ו-GRE.

♦ **L2TP** – מעביר UDP ביציאה 1701.

♦ **IPSec** – מעביר זיהוי פרוטוקול 50 ו-51 לצורך כותרת IPSec Authentication ומטען ESP מאוגד ומאובטח.

♦ **IP-IP** - מעביר זיהוי 4 של פרוטוקול IP.

❖ ודא כי לקוח Winsock Proxy אינו פעיל כרגע בלקוח VPN. כאשר לקוח Winsock Proxy פעיל, קריאות API של WinSock (כגון אלו המשתמשות ליצירת תעלה ולשליחת נתונים מתועלים) מתקבלות ומועברות לשרת Proxy המוגדר.

סיכום שיעור

VPN מחקה את מאפייני רשת ייעודית פרטית, ומאפשר לנתונים להיות מועברים בין שני מחשבים, דרך רשת ציבורית רחבת היקף, כגון האינטרנט. סניפי החברה יכולים להשתמש בשתי שיטות שונות כדי להתחבר לרשת דרך האינטרנט: שימוש בקווים ייעודיים, או שימוש בקווי חיוג. רשתות VPN משתמשות בתיעול לצורך העברת נתונים. תיעול (Tunneling) היא שיטה לשימוש בתשתית של רשתות רחבות היקף להעברת מטענים. פרוטוקול תיעול מכיל את פרוטוקול שימור התעלה ואת פרוטוקול העברת נתונים בתיעול. קיימים שני סוגים עיקריים של תיעול: תיעול רצוני (Voluntary Tunnel) ותיעול כפוי (Compulsory Tunnel). הפרוטוקולים העיקריים המשמשים את Windows 2000 לצורך גישה ל-VPN הם PPTP, L2TP, IPSec ו-IP-IP. כאשר מנהלים VPN יש לנהל משתמשים, כתובות ושרתי שמות, גישה, אימות והצפנה. אם אינך מצליח ליצור חיבור VPN, עליך לנסות ולפתור את הבעיה. איתור וטיפול בתקלות VPN הוא שילוב של איתור תקלות חיבוריות IP, יצירת חיבורי גישה מרחוק, ניתוב ו-IPSec.

שיעור 5: כלי RRAS

Windows 2000 כוללת קבוצת כלים, בהם תוכל להשתמש כדי לנהל ולאבחן תקלות RRAS. כלים אלה כוללים את תוסף התוכנה Routing and Remote Access, תוכנית שורת הפקודה netsh, ניהול יומני אימות וניהול חשבונות, ניהול יומני אירועים ועיקוב (Tracing).

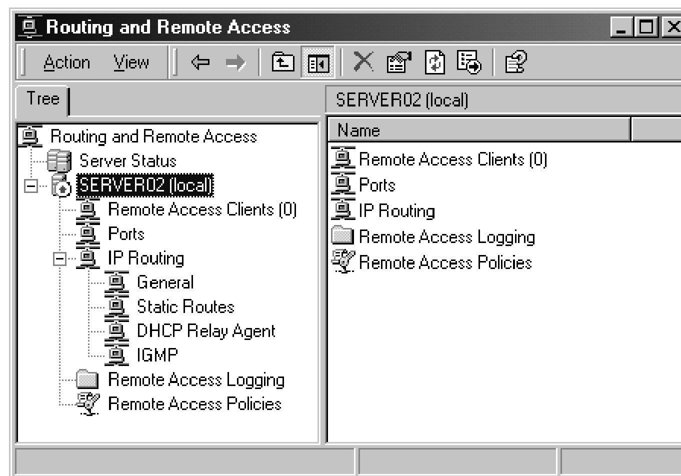
לאחר שיעור זה, תוכל

- להשתמש בכלים המסופקים עם Windows 2000, לניהול RRAS ולטיפול תקלות בו.

זמן לימוד משוער: 30 דקות

תוסף התוכנה של ניתוב וגישה מרחוק

תוסף התוכנה Routing and Remote Access מאפשר לך לבצע מיגוון משימות ניהול, כגון איפשור RRAS, ניהול ממשקי ניתוב, הגדרת ניתוב IPX, יצירת מאגר כתובות IP קבועות, הגדרת מדיניות גישה מרחוק וכדומה. למידע נוסף אודות תוסף התוכנה Routing and Remote Access, פתח אותו ולחץ על לחצן Help בחלון (תרשים 10.16).



תרשים 10.16 תוסף התוכנה Routing and Remote Access.

תוסף התוכנה Routing and Remote Access זמין בתיקיה Administrative Tools, והוא מהווה את כלי השירות העיקרי לניהול תצורת נתבים ושירותי גישה מרחוק של שרתי Windows 2000.

תוכנית השירות של
שורת הפקודה - Net Shell

Net Shell היא תוכנית שירות של שורת הפקודה עבור רכיבי רשת של Windows 2000 במחשבים מקומיים ומרוחקים. תוכנית השירות נקראת Netsh.exe, והיא מותקנת בתיקיה %systemroot%\System32 כאשר Windows 2000 מותקנת. Netsh גם מאפשרת שמירת תסריט תצורה (Configuration Script) כקובץ טקסט למטרות ארכיון, או כדי להגדיר שרתים נוספים.

Netsh יכולה לתמוך במספר מרובה של רכיבי Windows 2000 באמצעות סיפריות הקישור הדינמיות המסייעות לה (Helper DLL). ספריית קישור דינמית המסייעת ל- netsh, מרחיבה את אפשרויותיה על ידי אספקת פקודות נוספות לניטור והגדרת תצורה לרכיבי רישות מסוימים של Windows 2000. לדוגמה, Ippromon.dll הוא מסייע לשימוש בפקודות dhcp, dnsproxy, igmp, nat, ospf, dhcp relay ו-rip. כל DLL מסייע של netsh מספק הקשר (Context), קבוצת פקודות לרכיב רשת מסוים). בתוך כל הקשר יכולים להימצא הקשרי משנה. לדוגמה, בתוך ההקשר routing, נמצאים הקשרי המשנה ip ו-ipx המקבצים את פקודות ניתוב IP וניתוב IPX יחדיו.

הערה כל אפשרויות שורת הפקודה המתחילות בסימן מינוס (-) מופעלות מחוץ למצב המעטפת. מרגע שנכנסת למעטפת (Shell), פקודות מבוצעות ללא ציון netsh או סימן המינוס לפניהן.

אפשרויות שורת הפקודה של netsh כוללות:

- **-a <AliasFile>** מציין שניתן להשתמש בקובץ כינוי (Alias). קובץ כינוי מכיל רשימה של פקודות Netsh וגרסת כינוי, כך ששורת פקודה חלופית יכולה לשמש במקום פקודת Netsh. קבצי כינוי יכולים לשמש למיפוי פקודות לפקודת Netsh המתאימה, שיכולה להיות מוכרת יותר בפלטפורמות אחרות.
- **-c <Context>** מציין את ההקשר לפקודה מקבילה ב-DLL מסייע מותקן. לדוגמה, הפקודה:

```
netsh -c routing
```

מציבה אותך בהקשר של מסייע הניתוב.

- **Command** מציין איזו פקודת Netsh לבצע. ניתן להפעיל פקודות במצב המעטפת ומחוצה לו. לדוגמה:

```
netsh show helper
```

מציגה את המסייעים המותקנים בשורש המעטפת. לאחר הכניסה למעטפת על ידי הקלדת הפקודה netsh, תיראה הפקודה להצגת ה-DLL המסייעים המותקנים בשורש, כך:

```
show helper
```

- **-f <ScriptFile>** מציין שכל פקודות netsh שבקובץ התסריט יופעלו. לדוגמה, הפקודה:

netsh -f confgi.txt

מפעילה את כל התסריטים בקובץ config.txt.

- **-r <RemoteComputerName or IP_address>** מציין שפקודות Netsh מופעלות במחשב מרוחק, המוגדר על ידי שמו או על ידי כתובת IP. לדוגמה, הפקודה:

netsh -r RRAS2

מעבירה את Net Shell למצב פקודה עבור שרת RRAS ששמו RRAS2. מחוון שורת הפקודה משתנה, וכעת הוא ייראה כך:

[RRAS2] netsh>

ניתן לקצר את שמן של פקודות, עד למצב שהמחרוזת אינה משתמעת לשתי פנים. לדוגמה, אם תקליד במעטפת הפקודה את הפקודה ro ip sh int תהיה התוצאה זהה למצב בו תקליד את הפקודה routing ip show interface. פקודות Netsh יכולות להיות כלליות (גלובליות) או ייחודיות להקשר. פקודות כלליות יכולות להיות מופעלות בכל הקשר ומשתמשים בהן לפונקציונליות הכללית של Netsh. פקודות ייחודיות הקשר משתנות, בהתאם להקשר.

הטבלה הבאה מציגה את פקודות Netsh הכלליות.

פקודה	תיאור
..	עובר רמת הקשר אחת כלפי מעלה
help או ?	מציג עזרה של שורת הפקודה
add helper	מוסיף DLL מסייע של Netsh
delete helper	מוחק DLL מסייע של Netsh
show helper	מציג את ה- DLL המסייעים של Netsh שמותקנים
online	מגדיר את המצב הנוכחי למצב מקוון
offline	מגדיר את המצב הנוכחי למצב לא מקוון
set mode	מגדיר את המצב הנוכחי למצב מקוון או לא מקוון
show mode	מציג את המצב הנוכחי
flush	זונח את כל השינויים במצב לא מקוון
commit	מבצע את כל השינויים שנעשו במצב לא מקוון
set machine	מגדיר את המחשב בו תופעלנה פקודות Netsh

פקודה	תיאור
show machine	מציג את המחשב בו מופעלות פקודות Netsh
Exec	מפעיל קובץ תסריט המכיל פקודות Netsh
exit או bye או quit	יציאה מ- Netsh
add alias	מוסיף כינוי לפקודה קיימת
delete alias	מוחק כינוי מפקודה קיימת
show alias	מציג את כל הכינויים המוגדרים
dump	מעביר או מצרף תצורה לקובץ טקסט
popd	פקודת תסריטאות המקפיצה הקשר מהמחסנית
pushd	פקודת תסריטאות הדוחפת את ההקשר הנוכחי על המחסנית

ל-Netsh מצבי הפקודה הבאים:

- **Online** – במצב מקוון (Online), פקודות המופעלות משורת הפקודה של Netsh מבוצעות מייד.
- **Offline** – במצב לא מקוון (Offline), נאגרות פקודות המופעלות משורת הפקודה של Netsh, ומבוצעות כאצווה על ידי הפעלת פקודת ההפעלה Commit. ניתן להיפטר ממאגר הפקודות על ידי הפעלת הפקודה flush.

ניתן גם להפעיל קובץ תסריט (Script - קובץ טקסט המכיל רשימה של פקודות Netsh), על ידי השימוש במתג f- או על ידי הפעלת הפקודה Exec מתוך מעטפת Netsh.

כדי ליצור תסריט של התצורה הנוכחית הקלד את הפקודה הכללית **dump**. הפקודה dump מחוללת את התצורה הפעילה הנוכחית במונחים של פקודות Netsh. תוכל להשתמש בתסריט שיצרת באופן זה, כאשר אתה מגדיר שרת חדש, או כדי להגדיר מחדש את השרת הקיים. אם אתה מבצע שינויים נרחבים לתצורת רכיב כלשהו, מומלץ להתחיל את הגדרת הדו-שיח (session) עם הפקודה dump, למקרה שתצטרך לשחזר את התצורה לפני שאתה מבצע שינויים.

במקרה של RRAS יש ל-Netsh את ההקשרים הבאים:

- **ras** – השתמש בפקודות בהקשר ras כדי להגדיר תצורות גישה מרחוק.
- **aaaa** – השתמש בפקודות בהקשר aaaa כדי להגדיר תצורה של רכיב AAAA המשמש את Routing and Remote Access ואת Internet Authentication Service. AAAA מאחסן את הגדרות התצורה של שרת IAS.

- **routing** – השתמש בפקודה בהקשר routing כדי להגדיר ניתוב IP וניתוב IPX.
- **interface** – השתמש בפקודה בהקשר interface כדי להגדיר ממשקי חיוג-על-פי-דרישה.

למידע נוסף אודות פקודות ייחודיות הקשר, פנה למערכת העזרה של Windows 2000 Server ולעזרה המסופקת על ידי פקודת Netsh.

ניהול יומני אימות וניהול חשבונות

RRAS מאפשר ניהול יומן לנתוני אימות (Authentication) וניהול חשבונות (Accounting) לניסיונות התחברות מבוססי PPP, כאשר האפשרויות Windows Authentication או Accounting פעילות. רישומי יומן אלה נפרדים מרישומי היומן המבוצעים על ידי יומן אירועי המערכת (System Event Log). תוכל להיעזר בנתונים המופיעים ביומנים, כדי לעקוב אחר השימוש בגישה מרחוק וניסיונות האימות. רישום יומני האימות וניהול החשבונות יעיל במיוחד לטיפול בבעיות הקשורות למדיניות הגישה מרחוק. עבור כל ניסיון אימות נרשם שמה של מדיניות הגישה מרחוק אשר התקבלה או נדחתה.

נתוני האימות וניהול החשבונות מאוחסנים בקובץ יומן הניתן להגדרה, ואשר מאוחסן בתיקיה %systemroot%\System32\LogFiles. קבצי יומן נשמרים במבנה (פורמט) IAS גירסה 1.0 או במבנה מסד נתונים. משמעות הדבר היא שכל תוכנת מסד נתונים יכולה לקרוא קובץ יומן באופן ישיר, לצרכי אבחון.

תוכל להגדיר את סוג הפעילות שתירשם (פעולת ניהול חשבונות או אימות) ואת הגדרות קובץ היומן, כולל מיקום אחסון חלופי, ממאפייני התיקיה Remote Access Logging שבתוסף התוכנה Routing and Remote Access, או זה של Internet Authentication Service. מיקום רישום היומן מבוסס על הגדרות שבוצעו עבור ספק האימות וניהול היומן המשמשים את RRAS.

יומן אירועים

נתב Windows 2000 מבצע רישום שגיאות נרחב ביומן אירועי המערכת (System Event Log). תוכל להיעזר במידע זה כדי לאתר תקלות בניתוב או בתהליכי הגישה מרחוק ולטפל בהן.

קיימות ארבע רמות של רישום יומן:

- ❖ רישום שגיאות בלבד.
- ❖ רישום שגיאות ואזהרות.
- ❖ רישום כמות מירבית של נתונים.
- ❖ ביטול רישום יומן אירועים.

לדוגמה, אם נתב OSPF (**O**pen **S**hortest **P**ath **F**irst) אינו מצליח ליצור שכנות (adjacency) על ממשק, תוכל לפעול באופן הבא:

1. בטל (Disable) את OSPF בממשק.
2. שנה את רמת רישום היומן של OSPF, כך שתירשם כמות הנתונים המירבית.
3. אפשר (Enable) את OSPF בממשק.
4. בחן את יומן אירועי המערכת לנתונים אודות תהליך יצירת השכנות של OSPF.
5. שנה את רמת רישום היומן של OSPF, כך שיירשמו נתוני שגיאה בלבד.

אז, תוכל לאתר את בעיית יצירת השכנות של OSPF על ידי ניתוח הרשומות הקשורות בו ביומן אירועי המערכת.

את רמת רישום היומן ניתן לקבוע ממיגוון מקומות בתוסף התוכנה Routing and Remote Access. לדוגמה, ניתן לקבוע כי ינוהל יומן עבור מחשב מסוים בכרטיסיה Event Logging בתיבת דו-שיח של מאפייני אותו מחשב. תוכל גם לקבוע רישום יומן בתיבת הדו-שיח General Properties של IP Routing (בכרטיסיה General).

ניהול יומן צורך משאבי מערכת ורצוי להשתמש בו בצמצום, כדי לזהות בעיות ברשת. לאחר שהאירוע נרשם, או שהבעיה זוהתה, עליך מייד לשוב ולהגדיר את רישום היומן, כך שיירשמו בו שגיאות בלבד (Error Logging Only).

כאשר נרשמים ביומן מירב הנתונים, יכולים נתונים אלה להיות מורכבים ומפורטים עד מאוד. חלק מהנתונים הללו יכול להיות יעיל ביותר, אבל רק למהנדסי התמיכה של שירות התמיכה במוצר מטעם חברת Microsoft, או למנהלי רשתות אשר יש להם ניסיון רב בניתוב בסביבת Windows 2000.

Tracing

ל- RRAS של Windows 2000 יש יכולת נרחבת לביצוע עיקוב (Tracing), בה תוכל להיעזר כדי לאבחן בעיות חמורות ברשת. עיקוב רושם את המשתנים של רכיבים פנימיים, קריאות לפונקציות ואינטראקציות. רכיבי ניתוב וגישה מרחוק נפרדים יכולים להיות מאופשרים באופן פרטני, כך שירשמו נתוני יומן עיקוב לקבצים (File Tracing). עליך לאפשר פונקציות עיקוב על ידי שינוי הגדרות ברישום המערכת (Registry) של Windows 2000.

אזהרה אל תשתמש בעורך רישום (Registry Editor) כדי לערוך את רישום המערכת ישירות, אלא אם אין לך חלופות אחרות. עורכי רישום עוקפים את אמצעי הזהירות המסופקים על ידי כלי הניהול. אמצעי זהירות אלה מונעים ממך אפשרות לקבוע ערכים, העלולים לגרום להתנגשויות, או העלולים לגרום לירידה בביצועי המערכת, ואף לנזק. עריכה ישירה של הרישום יכולה לגרום לתוצאות בלתי צפויות וחמורות, אשר עלולות למנוע מהמערכת "לעלות", ולעיתים אף ידרשו התקנה מחדש של Windows 2000. כדי להגדיר או להתאים את Windows 2000, היעזר בתוכניות שבלוח הבקרה או בתוסף התוכנה, במידה והדבר אפשרי.

ניתן לאפשר עיקוב עבור כל אחד מפרוטוקולי הניתוב, על ידי עריכת ערכי רישום המערכת המתוארים בהמשך. תוכל גם לאפשר או לבטל את העיקוב אחר פרוטוקולי ניתוב בעת שהנתב פועל. כל פרוטוקול ניתוב או רכיב מותקן מסוגל לבצע עיקוב, ומופיע כמפתח (כגון OSPF ו- RIPV2).

עיקוב צורך משאבי מערכת ורצוי להשתמש בו בצמצום, כדי לסייע בזיהוי בעיות ברשת. לאחר שהעיקוב נלכד, או שהבעיה זוהתה, עליך מייד לבטל את העיקוב. אל תשאיר את העיקוב פעיל במערכות מרובות מעבדים (Multiprocessor Computers).

נתוני עיקוב עשויים להיות מורכבים ומפורטים עד מאוד. בדרך כלל יהיו נתונים אלה יעילים למהנדסי התמיכה של Microsoft או למנהלי רשתות, להם ניסיון רב בניתוב בסביבת Windows 2000.

קבצי עיקוב

כדי לאפשר קבצי עיקוב (File Tracing) לכל רכיב (מיוצג כ- Component בהמשך) עליך לשנות את הערך של רשומת רישום המערכת EnableFileTracing, שבמפתח הרישום HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Tracing\Component, מערך ברירת המחדל 0 (אפס) לערך 1 (אחד).

כדי לקבוע את מיקום קובץ העיקוב לכל רכיב, עליך לקבוע את הערך של רשומת רישום המערכת FileDirectory. מיקומו של קובץ העיקוב נרשם כנתיב. שם קובץ היומן הוא שם הרכיב שלגביו מוגדר העיקוב. כברירת מחדל, קבצי יומן נשמרים בתיקיה %systemroot%\Tracing.

כדי לקבוע את רמת קובץ העיקוב לכל רכיב, עליך לשנות את ערך רשומת רישום המערכת FileTracingMask. רמת העיקוב יכולה לנוע בין הערכים 0 (אפס) ועד 0xffff0000. כברירת מחדל נקבע ערך קובץ העיקוב כ-0xffff0000, רמת העיקוב המירבית.

כדי לקבוע את גודלו המירבי של קובץ העיקוב , עליך לשנות את ערך רשומת רישום המערכת MaxFileSize. ניתן לשנות את גודל קובץ היומן על ידי הגדרת ערכים שונים עבור MaxFileSize. ערך ברירת המחדל הוא 10000 (שהם 64KB).

סיכום שיעור

Windows 2000 כוללת קבוצת כלים, המאפשרת לך לנהל, לאתר תקלות RRAS ולטפל בהן. תוסף התוכנה Routing and Remote Access מאפשר לך לבצע מיגוון משימות ניהול, כגון אפשור RRAS, ניהול ממשקי ניתוב, הגדרת ניתוב IPX, יצירת מאגר כתובות IP קבועות, הגדרת מדיניויות גישה מרחוק וכדומה. Netsh היא תוכנית שירות ותסריטאות של שורת הפקודה עבור רכיבי רישות של Windows 2000, למחשבים מקומיים ומרוחקים. RRAS גם תומך ברישומי יומן אימות ונתוני ניהול חשבונות לניסיונות התחברות מבוססי PPP, כאשר האפשרויות Windows Authentication או Accounting מאופשרות. בנוסף, נתב Windows 2000 מבצע רישום יומן נרחב של שגיאות ביומן אירועי המערכת. תוכל להיעזר בנתונים שביומן אירועי המערכת כדי לנסות לאתר תקלות ניתוב או תקלות בתהליך הגישה מרחוק. RRAS של Windows 2000 כולל גם אפשרויות נרחבות של עיקוב, בהן תוכל להיעזר בעת הטיפול בתקלות רשת מורכבות.

שאלות סיכום

השאלות הבאות נועדו לחזק מידע מפתח שהוצג בפרק זה. אם אינך מסוגל לענות על שאלה סקור את השיעור המתאים ונסה לענות על השאלה פעם נוספת. תשובות לשאלות תמצא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואח״כ בעברית.

1. What is the purpose of demand- dial routing?
2. What authentication providers are available in RRAS and how are they different from authentication methods?
3. What is the purpose of VPN and what two VPN technologies are supported in Windows 2000 RRAS?
4. If a remote access client begins to connect to the RAS server but the connection is dropped, what troubleshooting steps will help you to solve this error?
5. How is the remote access permission of Deny Access (in Mixed mode or Native mode) , similar in function to the Native- mode domain default remote access policy?
6. You need to configure 10 RRAS servers for a client. All 10 servers will have identical RRAS configurations. What is the most efficient way to complete this configuration?

1. מהי מטרת ניתוב חיוג-על-פי-דרישה (Demand-Dial Routing)?
2. מי הם ספקי האימות (Authentication Providers) הזמינים ב-RRAS? במה הם שונים משיטות אימות (Authentication Methods)?
3. מהי מטרת VPN, וכיצד שתי טכנולוגיות VPN נתמכות ב-RRAS של Windows 2000?
4. אם לקוח גישה מרחוק מתחיל להתחבר לשרת RAS אבל החיבור ניתק, איזה צעדי איתור תקלה (Troubleshooting) יסייעו לך לפתור תקלה זו?
5. במה דומה הרשאת הגישה מרחוק Deny Access (במצב מעורב, Mixed Mode, או במצב טהור, Native Mode) לפעולת מדיניות ברירת המחדל של גישה מרחוק ל-Native-mode domain ?
6. עליך להגדיר עשרה שרתי RRAS עבור לקוח. בכל עשרת השרתים צריכות להיות הגדרות RRAS זהות. מהי הדרך היעילה ביותר לבצע את המשימה?

פרק 11

אמצעי אבטחת מידע בסביבת Windows 2000

אודות פרק זה

מערכת ההפעלה Windows 2000 מציגה מבנה מקיף של מפתח ציבורי (PKI - **P**ublic **K**ey **I**nfrastructure) לפלטפורמת Windows. PKI מרחיב את שירותי הקריפטוגרפיה של מפתח פרטי (PK), המבוססים על Windows, שהוצגו בשנים האחרונות, ומספקת קבוצת שירותים המשולבת בכלי ניהול המאפשרים ליצור, ליישם ולנהל יישומים מבוססי מפתח פרטי (PK-Based Applications). פרק זה מתאר את PKI של Windows 2000, דן בעיקרי טכנולוגיות המפתח הפרטי הנתמכות על ידי Windows 2000 ומספק מבט כללי אודות הפרוטוקולים Kerberos ו-IPSEC ב-Windows 2000. לסיום, מציג בפניך הפרק את כלי להגדרת תצורת אבטחת המידע והביקורת של Windows 2000, כלי בו תוכל להשתמש כדי לשמר את אבטחת המידע ברשת.

הערה אבטחת המידע ב-Windows 2000 היא קבוצה מתוחכמת ומקיפה של שירותים. למרות שנושא פרק זה הוא אבטחת המידע בסביבת Windows 2000, הוא אינו יכול להיכנס לעומקו של הנושא. אנו ממליצים לך לפנות למערכת העזרה של Windows 2000 ולאתר האינטרנט של Microsoft (בכתובת http://www.microsoft.com) כדי ללמוד עוד על נושא זה. בנוסף, בתקליטור המצורף לספר זה תמצא מספר מסמכי הסברה (White Paper). מסמכי הסברה אלה מכילים מידע מפורט אודות נושא האבטחה בסביבת Windows 2000. את המסמכים תמצא בתיקיה Chapt11\articles\.

לפני שתתחיל

לביצוע השיעורים בפרק זה נדרש:

- ❖ מחשב בו מותקנת ופועלת Microsoft Windows 2000.
- ❖ השלמת כל התרגילים בפרקים קודמים.

שיעור 1: מפתח ציבורי

קריפטוגרפיית מפתח ציבורי היא טכנולוגיה קריטית למסחר האלקטרוני (E-Commerce), רשתות אינטראנט (Intranet), אקסטראנט (Extranet) ויישומים Web אחרים. אבל, כדי לנצל את יתרונות קריפטוגרפיית המפתח הציבורי (Public Key) נדרשת תשתית תומכת. מערכת ההפעלה Windows 2000 כוללת Native Public Key Infrastructure, אשר תוכננה מראשיתה לנצל ניצול מלא את ארכיטקטורת אבטחת המידע של Windows 2000. שיעור זה מספק מבט כולל של PKI בסביבת Windows 2000 וכולל דיונים אודות מאפייני אבטחה, קריפטוגרפיה, אישורים (Certificates) ושירותי האישורים של Microsoft (Microsoft Certificate Services).

לאחר שיעור זה, תוכל

- לתאר את התפיסות הבסיסיות לגבי קריפטוגרפיית מפתח ציבורי ואת יישום PKI ב-Windows 2000.
- לעבד דרישות לאישורים ולהוסיף רשויות אישורים (**C**ertificate **A**uthorities - CAs).
- להתקין את שירותי האישורים של Microsoft (Microsoft Certificate Services).

זמן לימוד משוער: 35 דקות

מאפייני אבטחה

אבטחת מחשב כוללת הכל, החל בסביבת המחשוב הפיסית וכלה בסביבת התוכנה. בסביבה תוכנתית (Software Environment) צריכה אבטחה לספק ארבע פונקציות: אימות (Authentication), שלמות (Integrity), סודיות (Confidentiality) ומניעת הפעלה חוזרת (Anti-Replay).

Authentication

אימות (Authentication) הוא תהליך בו נקבעת אמינותו ומקוריות זהותו של מחשב או משתמש. אימות מבוסס על קריפטוגרפיה; הוא מבטיח שבעל כוונות זדון, המצותת לרשת לא יוכל להשיג את המידע הנדרש לשם התחזות למשתמש אמיתי או ליישות חוקית. הוא מאפשר ליישות מתקשרת להוכיח את זהותה ליישות אחרת, לפני שנתונים לא מאובטחים נשלחים דרך הרשת. ללא אימות תקיף, כל נתון והמחשב ממנו הוא נשלח נחשבים לחשודים.

Integrity

שלמות (Integrity) היא נכונות הנתונים, כפי שנשלחו במקור. שירותי שלמות מגינים על נתונים משינויים בלתי מורשים, המבוצעים בעת העברתם. ללא שלמות נתונים, כל נתון והמחשב ממנו הוא נשלח נחשבים לחשודים.

Confidentiality

סודיות (Confidentiality) מבטיחה כי הנתונים יגיעו רק לנמענים המיועדים.

Anti-Replay

מניעת הפעלה חוזרת (Anti-Replay), נקראת באנגלית גם Replay Prevention, מבטיחה כי צרורות נתונים (Datagrams) לא יישלחו פעם נוספת. ייחודיות זו מונעת התקפות מצד גורמים בעלי כוונת זדון, בהן הודעה נלכדת בדרכה ונשמרת, ואז נעשה בה שימוש חוזר במועד מאוחר יותר, כדי לבצע ניסיון גישה לא חוקי למידע. אם משתמש גלש לאתר האינטרנט של בנק ופעל שם בעזרת סיסמה ובסיום עבודתו סגר את הדפדפן, אז אף אחד אחר לא יוכל להכנס לחשבון דרך אפשרות "היסטוריה").

Cryptography

קריפטוגרפיה (Cryptography) היא קבוצת טכניקות מתימטיות להצפנה ופיענוח של מידע, כך שניתן יהיה לשלוח אותו באופן מאובטח ושהוא לא יילכד על ידי גורמים לא מורשים. קריפטוגרפיה עושה שימוש במפתחות, יחד עם אלגוריתמים לאבטחת מידע. מפתח (Key) הוא ערך שנועד להצפין או לפענח מידע. אפילו אם האלגוריתם ידוע לציבור, אין הדבר פוגע באיכות האבטחה, מפני שהנתונים אינם יכולים להיקרא ללא המפתח. לדוגמה, האלגוריתם של מנעול מספרים ידוע לכל: הגלגלים מוסטים בסדר מסוים כדי לפתוח את המנעול. אבל, המפתח למנעול - המספרים שהם הקוד - הוא סודי וידוע רק לאדם לו יש אותם. במילים אחרות, המפתח מספק את האבטחה, לא האלגוריתם. האלגוריתם מספק את התשתית בה מיושם המפתח. מערכות אבטחת מידע יכולות להיות מבוססות על קריפטוגרפיית מפתח ציבורי או מפתח פרטי, כפי שנראה בהמשך שיעור זה.

קיימים מספר אלגוריתמים ידועים לקריפטוגרפיה - כל אחד מהם תומך בפעילות אבטחה שונה.

הטבלה שלהלן מתארת מספר אלגוריתמי קריפטוגרפיה ידועים.

אלגוריתם	תיאור
RSA - **R**ivest, **S**hamir & **A**dleman	אלגוריתם למטרות כלליות אשר יכול לתמוך בחתימות דיגיטליות (Digital Signatures), אימות מבוזר (Distributed Authentication), הסכמי מפתח סודי באמצעות מפתח ציבורי (Secret Key agreement via Public Key) והצפנת נפח רב של נתונים ללא שיתוף סודות מקדים (Bulk data encryption without prior shared secrets). Shamir הוא הישראלי שבחבורה.
DSA - **D**igital **S**ignature Standard	אלגוריתם מפתח ציבורי, המשמש להפקת חתימות דיגיטליות.

אלגוריתם	תיאור
Diffie-Hellman	אלגוריתם קריפטוגרפיה של מפתח ציבורי, המאפשר לשתי יישויות מתקשרות להסכים על מפתח משותף, מבלי לדרוש הצפנה בעת חילול המפתח (Key generation).
HMAC - **H**ash **M**essage **A**uthentication **C**ode	אלגוריתם של מפתח סודי המספק שלמות, אימות ומונע הפעלה חוזרת. HMAC משתמש בפונקציות Hash משולבות במפתח סודי (Secret Key). Hash, הידוע גם כ- הודעת תקציר (Message Digest), משמש ליצירה ולווידוא חתימות דיגיטליות.
HMAC MD5 - **M**essage-**D**igest function **5**	פונקציית Hash המפיקה ערך בן 128 סיביות, הידוע כחתימה דיגיטלית (Digital Signature). החתימה משמשת לצורך אימות, שלמות ומניעת הפעלה חוזרת.
HMAC SHA - **S**ecure **H**ash **A**lgorithm	פונקציית Hash המפיקה חתימה דיגיטלית בת 160 סיביות, ומשמשת לצורך אימות, שלמות ומניעת הפעלה חוזרת.
DES-CBC - **D**ata **E**ncryption **S**tandard-**C**ipher **C**haining	אלגוריתם מפתח סודי המשמש לצרכי סודיות. באמצעותו מחולל (Generated) מספר אקראי המשמש, בשילוב עם מפתח סודי, להצפנת בלוק נתונים.

Public Key Cryptography

קריפטוגרפיית מפתח ציבורי (Public Key Cryptography) היא סכמה א-סימטרית, הנעזרת בזוג מפתחות לצורך הצפנה. השיטה נקראת א-סימטרית מפני שהיא נעזרת בשני מפתחות אשר מקורבים מבחינה מתימטית. מפתחות מקורבים אלה נקראים צמד מפתחות ציבורי ופרטי (Public and Private Key Pair). כדי להשתמש במפתח הציבורי לשם הצפנה, צריך האובייקט (למשל, משתמש) לחולל צמד מפתחות ציבורי ופרטי. האובייקט יחזיק רק מפתח פרטי אחד (זה שלו), אך יכול לשמור מספר רב של מפתחות ציבוריים המוצמדים למפתחות פרטיים אחרים. אובייקט משיג מפתחות ציבוריים באחת משתי הדרכים הבאות:

- בעליו של מפתח פרטי שולח למקבל מפתח ציבורי תואם.
- המקבל משיג את המפתח משירותי ספריית הרשת, כגון שירות Active Directory או מערכות DNS.

צמד מפתחות פרטי וציבורי משמשים בדרך כלל לשתי מטרות: הצפנת נתונים וחתימה דיגיטלית של הודעות (Digital Message Signing).

הצפנת נתונים

הצפנת נתונים מספקת סודיות, על ידי כך שהיא מבטיחה שרק הנמען הרצוי יוכל לפענח ולצפות בתוכן הנתונים המקוריים. כאשר יש צורך להעביר נתונים באופן מאובטח, משיג השולח את המפתח הציבורי של הנמען. השולח משתמש במפתח הציבורי של הנמען כדי להצפין את הנתונים, ואז שולח אותם. כאשר מקבל הנמען את

הנתונים המוצפנים, הוא משתמש במפתח הפרטי שלו כדי לפענח אותם. ההצפנה מאובטחת רק אם השולח משתמש במפתח הציבורי של הנמען לצורך ההצפנה. אם השולח משתמש במפתח הפרטי שלו לצורך הצפנת הנתונים, יכול כל אחד ללכוד את הנתונים ולפענח אותם, על ידי השגת המפתח הציבורי של השולח.

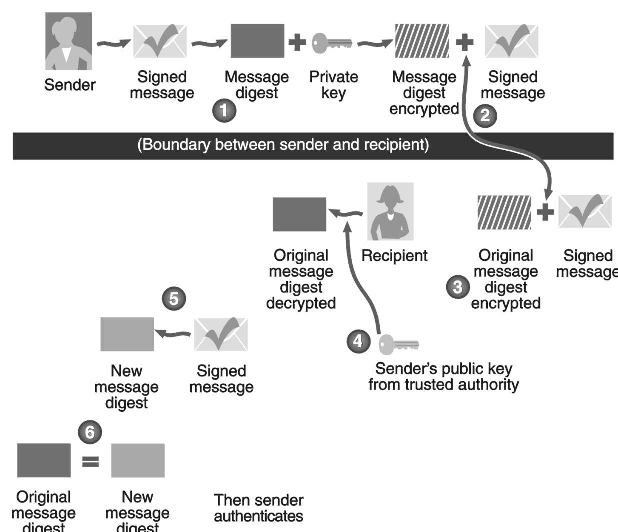
חתימה דיגיטלית של הודעות

חתימה דיגיטלית (Digital Signing) מספקת אימות ושלמות, אך אינה מספקת סודיות. חתימה דיגיטלית מאפשרת למקבל להיות בטוח בזהותו של השולח, ולוודא שתוכן ההודעה לא שונה בעת המעבר. דבר זה נועד כדי למנוע מהשולח לשלוח הודעות תוך התחזות למשתמש אחר.

כאשר שולח חותם את הודעתו נוצר תקציר הודעה (Message Digest). תקציר הודעה הוא ייצוג של ההודעה, ודומה ל-**C**yclic **R**edundancy **C**heck- CRC. השולח נעזר במפתח הפרטי שלו, כדי להצפין את תקציר ההודעה. כאשר הנמען מקבל את ההודעה, הוא משיג את המפתח הציבורי של השולח כדי לפענח את תקציר ההודעה. הנמען יוצר תקציר הודעה מההודעה השלמה, ואז משווה אותו עם התקציר המפוענח. אם תקצירי ההודעה זהים, מובטחת שלמות ההודעה (ראה תרשים 11.1).

לדוגמה, אתה מעוניין לרכוש ספר מאתר האינטרנט אמזון. באתר של אמזון אתה בוחר בדף רכישה בו עליך להכניס את נתוני העברת התשלום כגון מספר כרטיס אשראי. הנתונים בדף הרכישה מוצפנים עם המפתח הציבורי של חברת אמזון, כך שרק היא תוכל לפענח אותם באמצעות המפתח הפרטי של החברה.

כדי לוודא שדף הרכישה אכן נשלח על ידי חברת אמזון ולא חברה אחרת המתחזה לאמזון, נשלחת חתימה דיגיטלית המוצפנת עם המפתח הפרטי של אמזון ומאושרת על ידי צד שלישי מוסכם, המוסמך לתת אישורים (CA).



תרשים 11.1 השימוש בהודעה חתומה, תקציר הודעה והצפנת מפתח פרטי (PKI) כדי לוודא את אמיתות השולח.

אימות מסופק על ידי צמד המפתחות. מאחר שתקציר ההודעה הוצפן באמצעות המפתח הפרטי של השולח (ורק המפתח הציבורי של השולח יוכל לפענח את התקציר), יכול המקבל להיות בטוח שההודעה התקבלה מבעליו של צמד המפתחות. עם זאת, לשולח חייב להיות מנגנון כלשהו כדי להבטיח שצמד המפתחות אכן שייך לשולח הרצוי, ולא למישהו המתחזה להיות אותו משתמש. דבר זה מבוצע באמצעות אישור (Certificate) המופק על ידי צד-שלישי מוסכם, שמאשר את זהות בעליו של המפתח הציבורי. הצד-השלישי ידוע בשם רשות אישורים (**C**ertificate **A**uthority - CA), והוא יידון בהרחבה בהמשך שיעור זה.

מפתחות סודיים

מפתח סודי (Secret Key), הידוע גם כ- סוד משותף (Shared Secret) או כ- מפתח סודי משותף (Shared Secret Key), משמש בדרך דומה לזו בה משמש המפתח הציבורי; אולם, יש רק מפתח אחד המעניק אבטחה. מפתחות סודיים משמשים בדרך כלל רק לשיח מסוים או למשך זמן קצר, לפני שיופסק השימוש בהם. לתהליך זה יש יתרון על מפתחות ציבוריים. לדוגמה, אם אדם שאינו מורשה מצליח לשים ידו על המפתח הוא יוכל להתערב בשיח. אבל, אותו אדם זר לא יוכל להתחזות למשתמש או למחשב מחוץ לשיח, ולכן גם לא תהיה לו גישה למשאבים אחרים באמצעות המפתח הסודי.

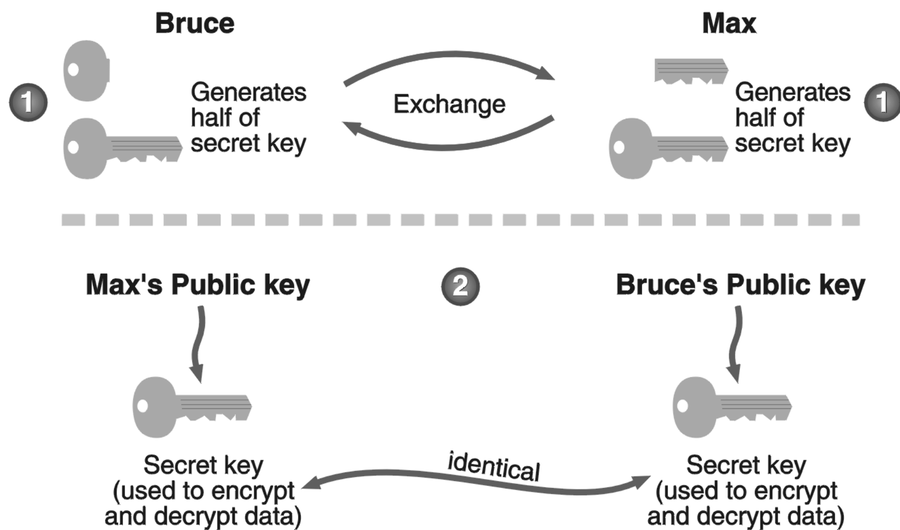
כדי ששני הצדדים יקבלו את המפתח הסודי המשותף, צריך להיות קיים מנגנון שיבצע זאת, מבלי להתפשר בנושא האבטחה. אם המפתח נשלח ברשת, תהיה למצותת (Eavesdropper) לרשת גישה קלה למפתח.

הערה מצותת (Eavesdropper) הוא מישהו המשתמש בכלי ניטור לרשת, ללכידת מנות העוברות בה.

חילופי מפתח סודי

הפתרון הנפוץ להספקת המפתח הסודי לשני הצדדים הוא על ידי שימוש במפתחות הציבוריים. מפתחות ציבוריים מאפשרים להצפין את המפתח הסודי, כאשר הוא נשלח ברשת. מפתחות ציבוריים מבטיחים סודיות, אימות ושלמות; בשל כך, אין כל פשרה בנושא אבטחת המידע כאשר המפתח הסודי נשלח.

לדוגמה, אם ברוס מעוניין לשלוח נתונים למקס, תוך שימוש במפתח סודי, יחולל כל אחד מהם את חציו של המפתח הסודי. ברוס ישיג את המפתח הציבורי של מקס כדי להצפין את חצי המפתח הסודי שלו, וישלח אותו למקס. ובדומה, מקס ישיג את המפתח הציבורי של ברוס, כדי להצפין את חצי המפתח הסודי שלו, וישלח אותו לברוס. אז, משלבים ברוס ומקס את שני חצאי המפתח, כדי לחולל את המפתח הסודי המשותף, שישמש אותם לצורך הצפנת הנתונים המיועדים לשליחה (תרשים 11.2). משא ומתן זה אודות המפתח הסודי, והשימוש במפתח הסודי לצורך הצפנת הנתונים, מספקים אימות, שלמות וסודיות.



תרשים 11.2 חילופי מפתח סודי, בהם מחוללים ברוס ומקס שני חצאי מפתחות אשר יחד ייצרו את המפתח הסודי המשותף להם.

הצפנת נתונים

כדי לספק סודיות, צריכים הנתונים להיות מוצפנים תוך שימוש במפתח סודי משותף. מכיון שקיים רק מפתח אחד הידוע לשני הצדדים, השולח והמקבל, תהליך ההצפנה ישר וקולע. מאחר שאף יישות אחרת ברשת אינה יודעת על קיומו של המפתח הסודי, הנתונים מוגנים בפני התקפה. בדרך כלל, השימוש במפתח הסודי המשותף פוסק מייד בתום השיח.

אישורים

הצפנה באמצעות מפתח ציבורי מניחה, שזהותו של בעל צמד המפתחות ברורה מעל לכל ספק. **אישור דיגיטלי** (Digital Certificate), אשר ניתן לקרוא לו בפשטות גם **אישור** (Certificate), הוא קבוצת נתונים המזהה זיהוי מוחלט את היישות המחזיקה בו. רשות מוסמכת להפקת אישורים (**C**ertification **A**uthority - CA) מפיקה אישורים, לאחר שהיא וידאה את זהות היישות. רשות האישורים היא גורם המוסכם על ידי שני הצדדים המתקשרים ביניהם.

לדוגמה, אם משה מעוניין לשלוח נתונים מאומתים לחיים, משה שולח את המפתח הציבורי שלו לחיים. רשות אישורים מאשרת את המפתח הציבורי של משה, ובכך גם מאשרת את זהותו של משה. מכיון שחיים סומך על רשות האישורים, הוא גם סומך על משה.

תהליך זה דומה לתפקידו של נוטריון ציבורי. אדם חותם על מסמך בפני נוטריון ציבורי ומספק לו הוכחה לגבי זהותו. הנוטריון הציבורי הוא יישות נסמכת, כך שכל מי שבוחן את המסמך יכול להיות בטוח שהחתימה היא אמיתית. בדומה לכך, כאשר שולח ההודעה חותם את הודעתו באמצעות המפתח הפרטי שלו, יכול המקבל להשתמש במפתח הציבורי, שנחתם על ידי רשות אישורים מוסמכת, כדי לוודא שהשולח הוא חוקי. מכיון שרשות אישורים מוסמכת מאשרת את המפתח הציבורי, יכול המקבל להיות בטוח שהשולח הוא מי שהוא מתיימר להיות. רשות אישורים מוסמכת יכולה להיות ספק אישורים צד-שלישי, כגון VeriSign או שירותי האישורים של Microsoft (Microsoft Certificate Services).

לדוגמה, משתמש יכול להשיג אישור דיגיטלי לשימוש בדואר האלקטרוני. האישור הדיגיטלי כולל את המפתח הציבורי ומידע אודות המשתמש. כאשר המשתמש שולח הודעת דואר אלקטרוני, כוללת ההודעה חתימה דיגיטלית, העושה שימוש במפתח הפרטי. הנמען מקבל את המפתח הציבורי, ומחליט אם שולח הודעת הדואר הוא השולח האמיתי. המפתח הפרטי לעולם אינו נשלח לנמען.

X.509

המונח X.509 מתייחס לתקן האיגוד הבינלאומי לטלקומוניקציה (ITU-T - **I**nternational **T**elecommunication **U**nion - **T**elecommunication) לתחביר ומבנה אישורים. תהליכים מבוססי-אישורים בסביבת Windows 2000 משתמשים בתקן X.509. מכיון שניתן להשתמש באישורים עבור יישומים שונים (למשל, דואר אלקטרוני מאובטח, הצפנת מערכת קבצים), בכל אישור כלול מידע שונה. אולם, על האישור לכלול את המאפיינים הבאים, לפחות:

- גירסה
- מספר סידורי
- מזהה אלגוריתם חתימה
- שם מפיק האישור
- תקופת תוקף
- שם הנושא (משתמש)
- נתוני המפתח הציבורי של הנושא
- מזהה ייחודי של המפיק
- מזהה ייחודי של הנושא
- סיומות
- חתימה על השדות המוזכרים לעיל

רשימות אישורים מבוטלים

תוקפם של אישורים, כמו לרוב סוגי האישורים בעולמנו, יכול לפוג, ואז אין לאישור כל תוקף. גם רשות האישורים יכולה לבטל את תוקפו של אישור מסיבות אלו ואחרות. כדי לטפל בקיומם של אישורים שאינם תקפים, שומרת רשות האישורים רשימת אישורים מבוטלים (**C**ertificate **R**evocation **L**ist - CRL). רשימת האישורים המבוטלים זמינה למשתמשי הרשת כדי לקבוע את תוקפו של כל אישור.

היררכיית רשות האישורים (CA)

במקום שתהיה רשות אישורים אחת בלבד עבור כל האינטרנט או האינטראנט, יכול להתקיים מצב בו רשויות אישורים מאשרות רשויות אישורים אחרות. מבנה היררכי זה, הנקרא שרשור, מאפשר למשתמשים לסמוך על רשות אישורים יחידה, במקום להידרש לסמוך על כל רשות אישורים הקיימת ברשת.

שרשור רשויות האישורים מספק את היתרונות הבאים:

- **גמישות** – קל להעביר, לבטל או לשרשר רשויות אישורים, מבלי לפגוע בחלקים אחרים של הארגון.
- **ניהול מבוזר** – מנהלי מערכות יכולים להיות אחראיים לאתרים שלהם.
- **מדיניות אבטחה** – מדיניות אבטחה יכולות להיות שונות בכל רשות אישורים.

רשות האישורים שברום השרשרת נקראת רשות השורש (Root CA), רשויות אישורים מתחתיה נקראות רשויות מתווכות (Intermediate), כפופות (Subordinate) או מנפקות (Issuing).

דוגמה: מדינת ישראל אחראית לכל האישורים הניתנים מתוקף המדינה ומוגדרת לצורך העניין כ- ISRAEL Root CA, אך כאשר אתה מעוניין לקבל אישור מוסמך כגון רשיון נהיגה או תעודת זהות אתה ניגש לרשויות שונות הכפופות למדינה. בדוגמה זו אתה ניגש למשרד התחבורה או משרד הפנים אשר דואגים להנפקת האישור המתאים מתוקף המדינה.

שירותי האישור של Microsoft

שירותי האישור של Microsoft (Microsoft Certificate Services) מאפשרים לארגון לנהל את ההפקה, החידוש והביטול של אישורים דיגיטליים מבלי שיצטרך לסמוך על רשות אישורים חיצונית. בנוסף, שירותי האישורים מאפשרים לארגון שליטה מלאה במדיניות המשויכות להפקת, ניהול וביטול אישורים, כמו גם את מבנה ותוכן האישורים עצמם. בנוסף, שירותי האישורים רושמים יומן אירועים של כל הפעולות המבוצעות, דבר המאפשר למנהל המערכת לעקוב, לבקר ולנהל בקשות להנפקת אישורים.

מאפייני שירותי האישור

לשירותי האישור של Microsoft יש מספר מאפיינים אשר הופכים אותם ליקרי ערך, עבור הארגון הבוחר שלא לסמוך על גורם חיצוני לצורך הנפקת אישורים, ואשר דורש כלי גמיש שיכול להיות מותאם לצרכי הארגון.

מדיניות עצמאית

כדי להשיג אישור, על המבקש לעמוד בקריטריונים מסוימים. קריטריונים אלה נקבעים במדינויות האישורים (Certificate Policies). לדוגמה, מדיניות אחת עשויה להעניק אישורים מסחריים, רק אם המבקש יציג את זיהויו באופן אישי. מדיניות אחרת עשויה להעניק אישור על סמך זיהוי המבוצע באמצעות דואר אלקטרוני.

מדינויות מיושמות ברכיבי מדיניות אשר יכולים להיכתב בשפת Visual Basic ,Java או Microsoft C/C++. מדיניות ברירת המחדל של שירותי האישור של Microsoft מאפשרת למשתמשים לבקש אישור באמצעות דף HTML.

העברה עצמאית

שירותי האישור יכולים לבקש ולהפיץ אישורים באמצעות כל מנגנון העברה קיים. זאת אומרת שהם יכולים לקבל בקשות לאישורים מהמבקש ולשלוח אליו את האישור באמצעות RPC ,HTTP (**R**emote **P**rocedure **C**all), קובץ דיסק או העברה מותאמת.

דבקות בתקנים

שירותי האישורים של Microsoft (Microsoft Certificate Services) יכולים לבצע את השירותים הבאים:

- לקבל בקשות **P**ublic **K**ey **C**ryptography **S**tandard #10 (PKCS) תיקניות
- לתמוך בנתונים החתומים בקריפטוגרפיית PKCS #7
- להפיק אישורי X.509 בגירסאות 1.0 ו- 3.0

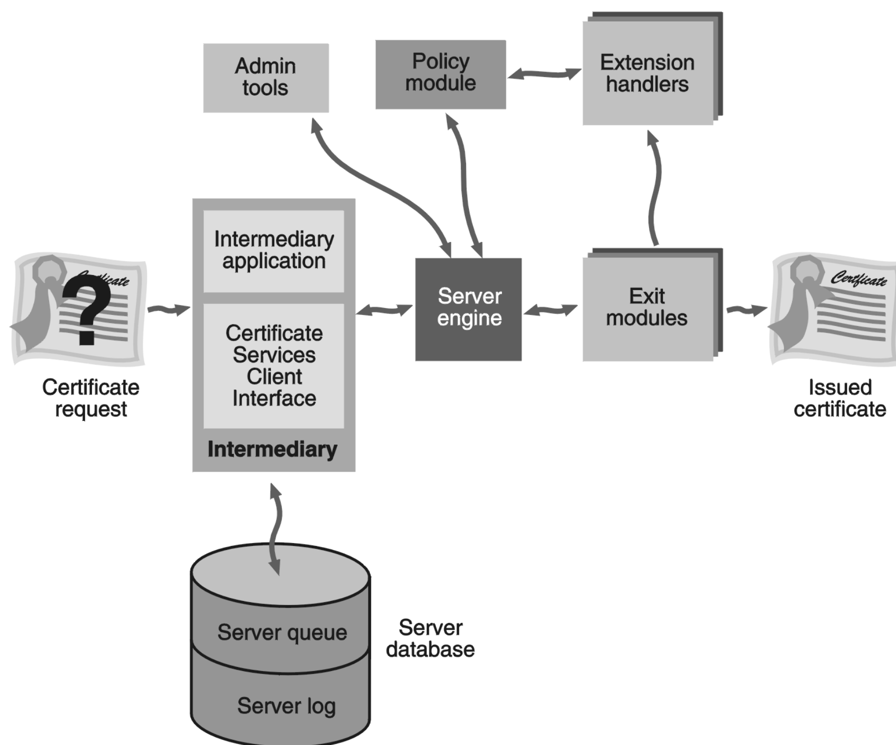
ניתן להוסיף לשירותי האישור תמיכה במבנה אישורים נוספים. שירותי האישור כוללים רכיב LDAP, כדי שיוכלו להיטמע בשירותי Active Directory.

ניהול מפתחות

אבטחת מערכת האישורים תלויה באבטחת המפתחות הפרטיים. עיצוב שירותי האישור מבטיח כי לא ניתן יהיה לגשת לנתוני המפתחות הפרטיים ללא הרשאה. שירותי האישור סומכים על Microsoft CryptoAPI שיספק את פונקציונליות ניהול המפתחות ואפשרויות קריפטוגרפיה נוספות, כדי ליצור מסד מאובטח, כאשר האישורים נשמרים ב-Certificate Store.

ארכיטקטורת שירותי האישור

מרכיבי ארכיטקטורת שירותי האישור כוללים את מנוע השרת המטפל בבקשות האישורים ומודולים נוספים, המבצעים משימות על ידי התקשרות עם מנוע השרת. תרשים 11.3 מתאר כיצד מתקשרים הרכיבים עם מנוע השרת.



תרשים 11.3 מנוע השרת ורכיבים אחרים של שירותי האישור.

מנוע שרת

מנוע השרת הוא רכיב הליבה של שירותי האישור (Certificate Services). המנוע פועל כמקשר (Broker) לכל הבקשות שהוא מקבל ממודולי רשומות. הוא מניע את שטף הנתונים בין הרכיבים, בעת עיבוד הבקשה והפקת האישור. בכל צעד בעיבוד מתקשר המנוע עם המודולים השונים, כדי להבטיח שהפעולה המתאימה ננקטת בהתאם למצב הדרישה.

מתווך

המתווך (Intermediary) הוא הרכיב הארכיטקטוני המקבל את הבקשות לאישורים חדשים מהלקוחות, ומגיש אותם למנוע השרת. המתווך מכיל שני חלקים: יישום המתווך, המבצע את הפעולות בשמו של הלקוח, וממשק הלקוח של שירותי האישור (Certificate Services Client Interface), המטפל בהתקשרויות שבין יישום המתווך ומנוע השרת.

יישומי מתווך יכולים להיכתב כך שיטפלו בבקשות אישורים מסוגים שונים של לקוחות, שיועברו דרך סוגים שונים של תווכי העברה או בהתאם לקריטריונים המוגדרים במדיניות. IIS (Microsoft **I**nternet **I**nformation **S**ervices) הוא יישום מתווך המספק ללקוחותיו תמיכה ב-HTTP. מתווכים יכולים גם לבדוק את מצבה של בקשה שהוגשה בעבר ולהשיג את נתוני תצורת שירותי האישור.

מסד נתוני שרת

שירותי אישור כוללים מסד נתוני שרת, השומר נתוני מצב (Status Information) ורושם ביומן את כל האישורים שהונפקו ואת רשימת האישורים שבוטלו (CRL). מסד הנתונים בנוי משני חלקים: יומן השרת (Server Log) ותור השרת (Server Queue).

Server Log

יומן השרת (Server Log) שומר את כל האישורים ורשימת האישורים המבוטלים שהונפקו על ידי השרת, כדי שמנהלי המערכת יוכלו לעקוב, לבקר ולשמור בארכיון את פעילות השרת. בנוסף, יומן השרת משמש את מנוע השרת כדי לאחסן ביטולים, מעט לפני שהם מפורסמים ברשימות האישורים המבוטלים (CRL). יומן השרת גם שומר למשך זמן מסוים (הניתן להגדרה) את הבקשות האחרונות לאישורים, למקרה שקרתה תקלה בעת הפקתו של אישור כלשהו.

Server Queue

תור השרת (Server Queue) שומר נתוני מצב (קבלה, ניתוח, הרשאה, חתימה ושיגור), בעת שהשרת מעבד בקשה לאישור, עד שהוא מתפנה לביצוע הפעולה.

מודול המדיניות

מודול המדיניות כולל קבוצת כללים השולטת בהפקה, חידוש וביטול של אישורים. כל הבקשות המתקבלות על ידי מנוע השרת מועברות למודול המדיניות, לשם מתן תוקף חוקי. מודולי מדיניות גם משמשים לניתוח כל נתון מוסף (Supplemental) המסופק עם הבקשה, ולקביעת מאפייני האישור בהתאם.

מטפלי סיומות

מטפלי סיומות (Extention Handlers) פועלים יחד עם מודולי המדיניות כדי לקבוע סיומות מותאמות לאישורים. כל מטפל סיומת פועל כתבנית לסיומות המותאמות שיכולות להופיע באישור. מודול המדיניות חייב לטעון את מטפל הסיומת המתאים כאשר הוא נדרש.

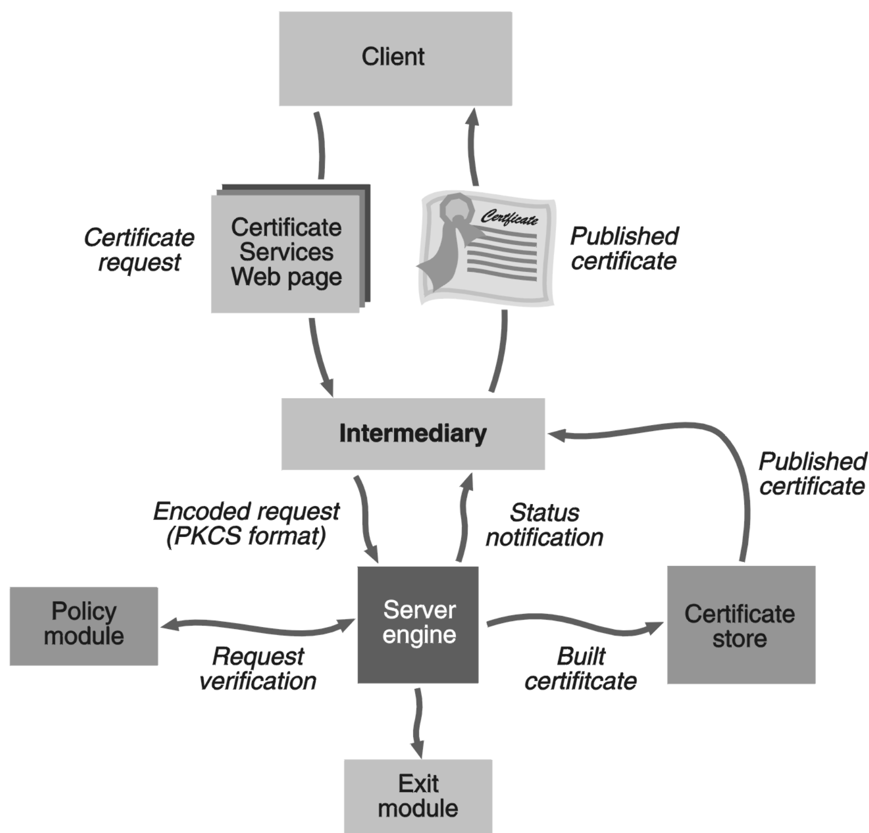
מודולי יציאה

מודולי יציאה מפרסמים אישורים מושלמים ורשימות אישורים מבוטלים (CRL), במיגוון אמצעי העברה ופרוטוקולים. כברירת מחדל, מודיע השרת לכל מודול יציאה המותקן בשרת, כאשר אישור מונפק או כשמפורסמת רשימת אישורים מבוטלים.

שירותי האישור מספקים ממשק COM (**C**omponent **O**bject **M**odel), לרישום מודולי יציאה מותאמים עבור סוגי העברה שונים ופרוטוקולים, או עבור אפשרויות מסירה מותאמות. לדוגמה, מודול יציאה של LDAP יכול לשמש לפרסום אישורי לקוחות בספריית הרשת (directory) בלבד, ולא אישורי שרתים. במקרה כגון זה, מודול היציאה יכול להיעזר בממשק COM, כדי לקבוע את סוג האישור שמנפיק השרת, ולסנן החוצה אישורים שאינם אישורי לקוח.

עיבוד בקשות לאישורים

שירותי אישור מספקים שירותים לעיבוד בקשות לאישורים, ומנפיקים אישורים דיגיטליים (ראה תרשים 11.4).



תרשים 11.4 עיבוד בקשות לאישורים.

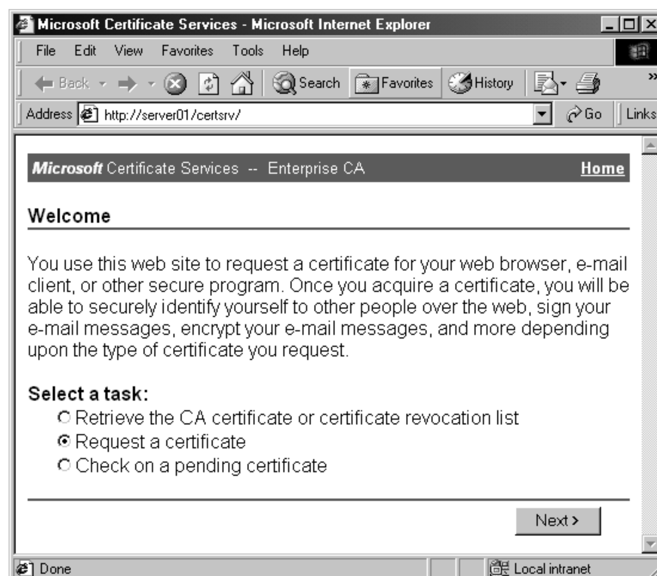
כשהם מעבדים בקשות לאישורים, מבצעים שירותי האישורים את הפעולות הבאות:

1. הבקשה לאישור נשלחת על ידי הלקוח ליישום מתווך. היישום המתווך מעצב את הבקשה למבנה בקשה PKCS #10, ומגיש אותה למנוע השרת.
2. מנוע השרת קורא למודול המדיניות, שמבצע שאילתה לגבי מאפייני הבקשה, קובע אם הבקשה מאושרת או לא, וקובע את מאפייני הבקשה האופציונליים.
3. אם הבקשה מאושרת, לוקח מנוע השרת את הבקשה ובונה עבורה אישור מושלם.
4. מנוע השרת מאחסן את האישור המושלם במחסן האישורים, ומיידע את יישום המתווך אודות מצב הבקשה. אם מודול היציאה ביקש זאת, מודיע לו מנוע השרת לגבי אירוע הנפקת האישור. הודעה זו מאפשרת למודול היציאה לבצע פעולות נוספות, כגון פירסום האישור בשירותי ספריית הרשת (כגון Active Directory).
5. המתווך מקבל את האישור המונפק ממסד האישורים, ומעביר אותו אל הלקוח שדרש אותו.

רישום אישורים

תהליך השגת אישור דיגיטלי נקרא **רישום לאישור** (Certificate Enrollment). התהליך מתחיל בכך שהלקוח מגיש בקשה לקבלת אישור, ומסתיים בהתקנת האישור ביישום הלקוח.

בקרת הרישום והטפסים שלה נגישים מהדף Certificate Services Enrollment Page. דף זה זמין מתוך דף ה-Web של שירותי האישור (Certificate Services) בכתובת http://server_name/certsrv/.



תרשים 11.5 טופס בקשת רישום עבור Server01, המוגדר כרשות אישורים ארגונית (Enterprise CA).

אישורים של CA

בתהליך הנפקת אישור דיגיטלי, בוחנת רשות האישורים את זהות המבקש, ואז חותמת על האישור באמצעות המפתח הפרטי שלה.

יישום לקוח, כגון Internet Explorer של Microsoft, בוחן את חתימת רשות האישורים, לפני שהוא מקבל את האישור. אם תוקף חתימת הרשות פג, או שמקורו לא ידוע, Internet Explorer מזהיר את המשתמש על ידי הצגת הודעת אבטחה (Security Message), והוא אף עשוי למנוע מהמשתמש לקבל את האישור.

הערה אם Internet Explorer מוגדר לרמת אבטחה נמוכה (Low Security Level), הוא לא יזהיר את המשתמש בפני אישורים שאינם תקפים. הגדרה שכזו מתאימה רק לסביבות אינטרנט בטוחות לחלוטין, אך אינה מתאימה לגישה לאינטרנט.

בנוסף לאישורי האימות של השרת ושל הלקוח, המונפקים על ידי שירותי האישור, קיימים גם אישורים המזהים רשויות אישורים.

אישור רשות אישורים הוא אישור חתימה, המכיל מפתח ציבורי שמשמש לווידוא חתימות דיגיטליות. הוא מזהה את רשות האישורים אשר הנפיקה אישורי אימות (Authentication Certificate) לשרתים ולקוחות המבקשים אישורים כאלה. לקוחות משתמשים באישורי רשות אישורים אשר הנפיקה את אישור השרת, כדי לאמת את אישור השרת. שרתים משתמשים באישור רשות האישורים, כדי לאמת את אישורי הלקוח.

אישור רשות אישורים החתום חתימה עצמית (Self-Signed) נקרא גם **אישור שורש**, מפני שהוא האישור לשורש רשות האישורים (Root CA). שורש רשות האישורים חייב לחתום את האישור של עצמו, מכיון שעל פי ההגדרה לא קיימת רשות אישור גבוהה ממנו, שיכולה לחתום את אישור רשות האישורים שלו.

הפצה והתקנה של אישורי רשות אישורים (CA)

אישורי רשות אישורים אינם מבוקשים ומונפקים באותו אופן בו מונפקים אישורי אימות של שרת ושל לקוח. אישורי אימות של שרת ושל לקוח הם ייחודיים לכל שרת או לקוח המבקש אותם, והם אינם משותפים - יש לחולל אותם ולהנפיק אותם על-פי דרישה. בניגוד לכך, אישור של רשות אישורים אינו דורש הנפקה על-פי דרישה. במקום זאת, הוא נוצר פעם אחת, ואז הופך לזמין לכל השרתים והלקוחות המבקשים אישור של רשות אישורים.

טכניקת הפצה מקובלת לאישורי רשות אישורים היא להציב אותם במיקום ידוע ונגיש, לכל מי שמבקש אישור מסוג זה.

התקנת שירותי אישור

תוכל להתקין את שירותי האישור (Certificate Services) באמצעות היישומון Add/Remove Programs שבלוח הבקרה, או כאפשרות במהלך תהליך ההתקנה של Windows 2000 Server. מנהלי מערכות, המכירים את נושא יצירת רשויות אישורים, יכולים לבחור התקנה מותאמת, על ידי בחירה באפשרויות המתקדמות הזמינות בעת התקנת שירותי האישור. אלה שאינם מכירים את אופן יצירת רשות אישורים יכולים לבחור בהגדרות ברירת המחדל.

סוג רשות אישורים (CA)

סוג CA מאפשר בחירה, כיצד תנוצל הרשות בהיררכיית רשויות האישורים ואם רשות האישורים תסתמך על שירותי Active Directory או לא. סוגי רשויות האישורים הבאים זמינים:

- **Enterprise Root CA** – רשות אישורים זו הופכת לרשות השורש עבור ההיררכיה, ודורשת את שירותי Active Directory.
- **Enterprise Subordinate CA** – רשות אישורים זו הופכת לרשות כפופה לרשות שורש (Enterprise Root CA). היא דורשת שירותי Active Directory, ותבקש הנפקת אישור מרשות השורש.
- **Stand-alone Root CA** – רשות אישורים זו הופכת לרשות השורש עבור ההיררכיה, אך אינה דורשת את שירותי Active Directory.
- **Stand-alone Subordinate CA** – רשות אישורים זו הופכת לרשות כפופה לרשות שורש (Stand-alone Root CA). היא אינה דורשת שירותי Active Directory, ותבקש הנפקת אישור מרשות השורש שלה (Stand-alone Root CA).

כאשר מתקינים את רשות האישורים כ- Enterprise CA, מעתיקים שירותי האישורים את האישורים לתוך שירותי Active Directory. ספקי אבטחה, כגון Kerberos, יכולים לבצע שאילתה בשירותי Active Directory, כדי לקבל את האישור אשר מכיל את המפתח הציבורי.

נתוני CA

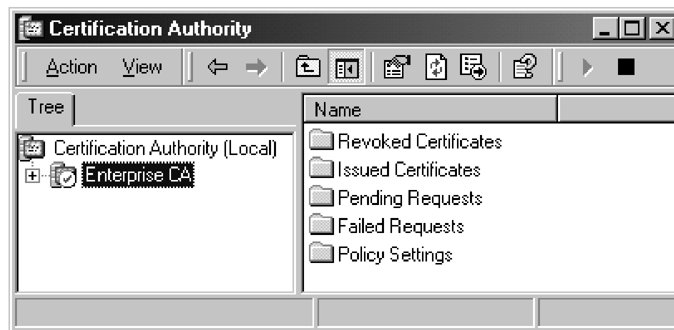
כאשר אתה מתקין את שירותי האישור (Certificate Services), עליך לספק נתונים אודות רשות האישורים הראשונה הנוצרת. הנתונים כוללים את שם הרשות ונתונים נחוצים נוספים. לאחר שתהליך התקנת CA הושלם, אין אפשרות לשנות את הנתונים הללו.

הגדרות מתקדמות

חלק ההגדרות המתקדמות (Advanced Configuration) כולל מספר אפשרויות, לגבי סוג אלגוריתם הקריפטוגרפיה, בו ייעשה שימוש ב-CA שאתה יוצר. אפשרויות ההגדרה המתקדמות כוללות את שם ספק הקריפטוגרפיה, אלגוריתם Hash, האפשרות להשתמש במפתחות פרטיים וציבוריים קיימים ואורך המפתח.

ניהול שירותי אישורים

הכלי הראשי המשמש לניהול שירותי אישורים הוא תוסף התוכנה Certification Authority (ראה תרשים 11.6).



תרשים 11.6 תוסף התוכנה Certification Authority עבור Enterprise CA.

תוסף תוכנה זה מאפשר ביצוע מיגוון משימות ניהול:

- להפעיל ולעצור את שירות CA
- לקבוע הרשאות אבטחה ולהאציל שליטה ב-CA
- לצפות באישור CA
- לגבות CA
- לשחזר CA מעותק גיבוי
- לחדש CA שורש
- לחדש CA כפופה
- לנהל ביטול אישורים
- לנהל בקשות לאישורים
- לנהל תבניות אישורים
- לשנות הגדרות מדיניות
- למפות אישורים לחשבונות משתמש
- לשנות את מודול המדיניות ואת מודול היציאה

תוכל להשתמש בתוסף התוכנה Certification Authority, כדי לנהל רשות אישורים במחשב המקומי או במחשב אחר. תוסף התוכנה מותקן, כאשר מותקנים שירותי האישורים, או כאשר מתקינים את ערכת הניהול (Administration Pack, Adminpak.msi).

Certutil.exe היא תוכנית שירות של שורת הפקודה המשמשת לניהול שירותי אישורים. הפעלת הפקודה ללא מתגים תציג תקציר של רשות האישורים המקומית. Certutil משמשת להשלכת נתוני תצורת CA ולהצגתם, להגדרת שירותי אישורים (Certificate Services), גיבוי ושחזור רכיבי CA ולשם וידוא אישורים, צמדי מפתחות ושרשרות אישורים.

אם אתה צריך להגדיר אבטחה עבור דפי ה-Web של CA, עליך להשתמש בתוסף התוכנה Internet Information Services. בחלון Tree הרחב את הצומת Default Web Site ובחר ב-CertSrv. מתפריט Action בחר Properties. בכרטיסיה Directory Security, בתיבה Anonymous access and authentication control לחץ Edit. בתיבת הדו-שיח Authentication Methods קבע את הגדרות האבטחה עבור דפי ה-Web של CA.

תרגיל 1 : התקנה והגדרה של שירותי אישורים

בתרגיל זה תתקין Enterprise Root CA ותיעזר בה כדי להנפיק, להתקין ולבטל אישורים. שים לב לכך שהאופן הבטוח להגדרת Certificate Services הוא על ידי יצירת CA שורש, המנפיקה אישורים אך ורק לרשויות מסוג CA כפופות. אז מנפיקה ה-CA הכפופה אישורים למטרות מסוימות, כגון שירותי יישומים ואימות. השימוש ב-CA שורש למטרה זו אינו בטוח, מכיון שאם נפרצת אבטחת CA השורש, כל האישורים המונפקים על ידה אינם מאובטחים יותר. אולם, כדי שתלמד כיצד להתקין ולהגדיר שירותי אישורים, נשתמש ב-CA שורש.

הליך 1 : התקנת Certificate Services והגדרת Certification Authority

בהליך זה תתקין את שירותי האישורים (Certificate Services) ב-Server01. Server01 יתפקד כ- Enterprise Root CA.

1. היכנס למחשב Server01 בשם משתמש Administrator ועם הסיסמה password.
2. לחץ Start, הצבע על Settings ובחר Control Panel. חלון לוח הבקרה יופיע.
3. לחץ לחיצה כפולה על Add/Remove Programs. חלון Add/Remove Programs יופיע.
4. בחלונית השמאלית, לחץ על הסמל Add/Remove Windows components. חלון אשף Windows Components יופיע.
5. סמן את תיבת הסימון Certificate Services.

   תופיע תיבת הודעה, לה הכותרת Microsoft Certificate Services. תיבה זו מודיעה כי מרגע ששירות האישורים יותקן במחשב זה, לא ניתן יהיה לשנות את שם המחשב, ולא ניתן יהיה לצרפו או להעבירו ל-Domain.
6. לחץ Yes.

7. במסך Windows Components לחץ על Details. מסך Certificate Services יופיע.

שים לב שרכיבי המשנה של שירותי האישורים כוללים גם את השירות המשמש ליצירת רשות אישורים (CA) וגם טופס Web להרשמה, לצורך הגשת בקשה וקבלת אישורים ממחשב המתפקד כ-CA.

8. לחץ OK.

9. במסך Windows Components לחץ Next. המסך Certification Authority Type יופיע.

10. בחר בכל אחד מלחצני האפשרויות, וקרא את הטקסט המופיע בתיבה Description.

שים לב שהסוג Enterprise CA יכול לשמש רק אם שירותי Active Directory פעילים. סוגי Stand-alone CA יכולים לפעול באופן עצמאי משירותי Active Directory. בשל כך, ניתן להשתמש בהם, כאשר אין שירותי Active Directory פעילים, או כאשר שירותים אלה פעילים. אם קיימים שירותי Active Directory, ישתמשו בהם סוגי Stand-alone CA. סוגי Subordinate CA תלויים בהימצאותה של רשות אישורים ברמה גבוהה יותר של היררכיית הרשויות.

11. לחץ על לחצן האפשרויות Enterprise Root CA, וסמן את תיבת הסימון Advanced Options.

12. לחץ Next. יופיע המסך Public and Private Key Pair.

שים לב לכך שקיימים מספר ספקי שירותי קריפטוגרפיה (CSP - **C**ryptograpic **S**ervice **P**rovider), כאשר לכל אחד מהם משויך אלגוריתם Hash, אחד או יותר, המשמש לחילול צמד המפתחות. ממסך זה תוכל גם לציין את אורך המפתח, או להשתמש במפתחות הקיימים המותקנים במחשב, לייבא מפתחות ולצפות באישורים.

13. בתיבת הרשימה CSP, ודא כי נבחרה האפשרות Microsoft Base Cryptographic Provider v1.0. בתיבת הרשימה Hash Algorithm, ודא כי נבחר אלגוריתם Hash מסוג SHA-1. מתיבת הרשימה הנפתחת Key Length, ודא כי נבחרה האפשרות Default. לחץ Next. יופיע המסך CA Identifying Information.

14. הקלד את הנתונים המופיעים בטבלה הבאה לתיבות הטקסט המתאימות שבמסך CA Identifying Information.

תווית	ערכים להקלדה
CA Name	Enterprise CA
Organization	Microsoft Corporation
Organizational Unit	Microsoft Press
City	Redmond
State or Province	Washington
E-Mail	ca-mp@microsoft.com
CA description	Root CA for self study training only

שים לב שאישור זה מוגדר להיות חוקי למשך תקופה של שנתיים.

15. לחץ Next. יופיע המסך Data Storage Location.

שים לב שהתיקיה בה מאוחסנים מסד נתוני האישורים וקובץ היומן, CertLog, נוצרת במחיצת האתחול (Boot Partition). אם הנפח הפנוי במחיצת האתחול מצומצם, רצוי להגדיר מחיצה מאובטחת אחרת לשמירת קבצים אלה.

האפשרות Store configuration information in a shared folder אינה נחוצה אם שירותי Active Directory פעילים, ואם המחשב המתפקד כרשות אישורים הוא חבר ב-domain. נתוני תצורה אודות CA מפורסמים באופן אוטומטי ב-Active Directory.

16. לחץ Next. תיבת הודעה שכותרתה Microsoft Certificate Services מופיעה, ומציינת כי Internet Information Services פעילים במחשב, ומזהירה אותך כי הם חייבים להיות מופסקים כדי שתוכל להמשיך.

17. לחץ OK. בעת שהתוכנה מותקנת ומוגדרת מופיע המסך Configuring Components, ואחריו מופיע המסך Completing the Windows Components Wizard.

18. לחץ Finish, ובחלון Add/Remove Programs לחץ Close.

19. סגור את לוח הבקרה.

הליך 2: הפעלת Certificate Services

בהליך זה תחולל, תתקין ותבטל אישור במחשב Server01. תשתמש בכתובת ה-URL של Certificate Enrollment ובתוסף התוכנה Certification Authority, כדי להשלים הליך זה.

1. לחץ Start, הצבע על Programs ומהקבוצה Administrative Tools בחר באפשרות Certification Authority. יופיע תוסף התוכנה Certification Authority.
2. בחלון Tree, הרחב את הצומת Enterprise CA.
3. בחלון Tree, בחר בתיקיה Issued Certificates, ומזער את חלון תוסף התוכנה Certification Authority.
4. לחץ Start ובחר Run. תיבת הדו-שיח Run תופיע.
5. בתיבת הטקסט Open הקלד **http://server01/certsrv** ולחץ OK. יופיע האשף Internet Connection.
6. בחר בלחצן האפשרויות I want to setup my internet connection manually, או ב- I want to connect through a local area network (LAN).
7. לחץ Next. יופיע המסך Setting up your internet connection.
8. לחץ על לחצן האפשרויות I connect through a local area network (LAN).
9. לחץ Next. יופיע המסך Local area network internet connection.
10. בטל את הסימון בתיבת הסימון Automatic Discovery of Proxy Server (Recommended).
11. לחץ Next. יופיע המסך Set up your internet mail account.
12. סמן את לחצן האפשרויות No ולחץ Next.

    יופיע המסך Completing the Internet Connection Wizard.
13. לחץ Finish. Internet Explorer יופיע ויציג את דף ההרשמה של שירותי האישורים.
14. קרא את המידע המופיע בדף זה, וודא שלחצן האפשרויות Request a certificate נבחר.
15. לחץ Next. יופיע הדף Choose request type ובו נבחר לחצן האפשרויות User certificate request.
16. לחץ Next. יופיע הדף User Certificate - Identifying Information.
17. לחץ על More Options. שים לב שה-CSP הנבחר הוא סוג ה-CSP שבחרת בעת ההתקנה של שירותי האישורים.
18. לחץ על Submit. יופיע הדף Certificate Issued.

19. מזער את Internet Explorer, ושחזר את חלון תוסף התוכנה Certification Authority.

תוסף התוכנה Certification Authority יופיע ואישור אחד יהיה רשום בחלונית הפרטים. אם אינך רואה את הבקשה לאישור, הקש F5 כדי לרענן את החלונית.

20. לחץ לחיצה כפולה על האישור המופיע בחלונית הפרטים. תופיע תיבת הדו-שיח Certificate ובה שלוש כרטיסיות.

21. בחר בכרטיסיה Details.

22. בתיבה העליונה, מתחת לתיבת הרשימה הנפתחת Show, לחץ על Issuer.

שים לב שהמידע המופיע בתחתית התיבה, הוא המידע אותו הקלדת במסך CA Identifying Information בשלב 14 של הליך 1.

23. לחץ OK.

24. מזער את חלון תוסף התוכנה Certificate Authority, ושחזר את חלון Internet Explorer.

25. לחץ על הקישור Install this certificate. יופיע הדף Certificate Installed, ובו מצוין כי האישור הותקן בהצלחה.

26. סגור את חלון Internet Explorer.

27. שחזר את חלון תוסף התוכנה Certificate Authority, ובחר באישור שבחלונית הפרטים.

28. פתח את תפריט Action, הצבע על All Tasks, ובחר Revoke Certificate.

תופיע תיבת הדו-שיח Certificate Revocation.

29. מתיבת הרשימה הנפתחת Reason Code, בחר Key Compromise, ולחץ Yes.

30. בחלון Tree, לחץ על התיקיה Revoked Certificates. האישור המבוטל יופיע בחלונית הפרטים.

31. פתח את תפריט Action, הצבע על All Tasks, ובחר Publish.

תופיע תיבת הדו-שיח Certificate Revocation list, המציינת כי הרשימה הקודמת עדיין תקפה.

32. לחץ Yes.

33. סגור את תוסף התוכנה Certificate Authority.

34. לחץ Start ובחר Run. תופיע התיבה Run וכתובת ה-URL של CertServ רשומה בה.

35. לחץ OK. Internet Explorer יופיע ויציג את דף ההרשמה לשירותי האישורים.

36. לחץ על לחצן האפשרויות Retrieve the CA Certificate or Certificate Revocation List, ולחץ Next.

37. לחץ על הקישור Download Latest Certificate Revocation List. תופיע תיבת הדו-שיח File Download.

38. לחץ על לחצן האפשרויות Open this file from its current location, ולחץ OK.

תופיע תיבת הדו-שיח Certificate Revocation List.

39. בחר בכרטיסיה Revocation List.

40. לחץ על הפריט המופיע בתיבה Revoked Certificates.

בתיבת הרשומה Revocation מופיעים המספר הסידורי של האישור המבוטל, תאריך הביטול והסיבה לביטול.

41. לחץ OK.

42. סגור את חלון Internet Explorer.

סיכום שיעור

Windows 2000 כוללת PKI (**P**ublic **K**ey **I**nfrastructure) טבעי, אשר מיועד לנצל במלואה את ארכיטקטורת אבטחת המידע של Windows 2000. קריפטוגרפיית המפתח הפרטי היא סכמה א-סימטרית, הנעזרת בצמד מפתחות לצורך ההצפנה. כדי להשתמש בהצפנת מפתח ציבורי, חייב המשתמש לחולל צמד מפתחות, ציבורי ופרטי. הצפנת מפתח ציבורי נעזרת באישורים דיגיטליים לזיהוי מוחלט של בעל צמד המפתחות. התהליך מבוסס-האישור של Windows 2000 משתמש בתקן X.509. שירותי אישורים (Certificate Services) מאפשרים לארגון לנהל בעצמו את הנפקת, חידוש וביטול אישורים דיגיטליים, מבלי להסתמך על רשויות אישורים (CA) חיצוניות. שירותי אישורים תומכים במדיניות עצמאית, העברה עצמאית, דבקות בתקנים וניהול מפתחות. רכיבי ארכיטקטורת שירותי האישורים כוללים את מנוע השרת (Server Engine), המטפל בבקשות לאישורים, ומודולים נוספים המבצעים משימות על ידי התקשרות עם מנוע השרת. שירותי האישורים מספקים שירותים לעיבוד בקשות לאישורים ולהנפקת אישורים דיגיטליים. ניתן להתקין את שירותי האישורים באמצעות היישומון Add/Remove Programs שבלוח הבקרה, או כאפשרות בעת התקנת שרת Windows 2000. הכלים המשמשים לניהול שירותי האישורים לאחר שהם מותקנים, הם תוסף התוכנה Certificate Authority ודף ה-Web להרשמה (Certificate Services Enrollment Web page).

שיעור 2:
טכנולוגיות המפתח הציבורי

Windows 2000 מרחיבה את נושא אבטחת המידע, באמצעות תמיכה במספר טכנולוגיות המבוססות על אבטחת המפתח הציבורי, כולל חבילת אימות ערוץ מאובטח (Secure Channel authentication package), כרטיסים חכמים (Smart Cards), Authenticode, מערכת הקבצים המוצפנת (**E**ncrypted **F**ile **S**ystem - EFS) ופרוטוקול האבטחה של האינטרנט (**I**nternet **P**rotocol **Sec**urity - IPSec). שיעור זה סוקר כל אחת מהטכנולוגיות המוזכרות ומסביר כיצד הן מתאימות למסגרת פעולתה של תשתית המפתח הציבורי (**P**ublic **K**ey **I**nfrastructure - PKI).

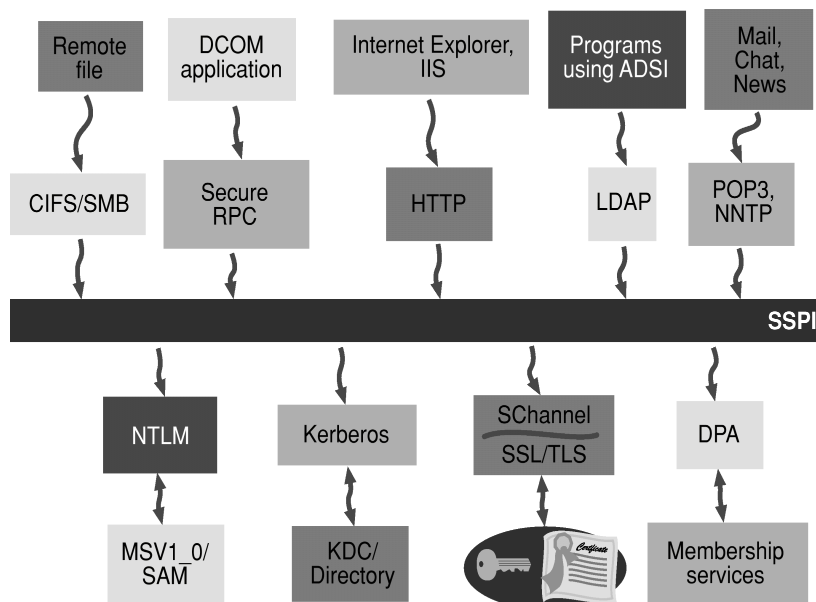
לאחר שיעור זה, תוכל

- לתאר את הרכיבים העיקריים של אבטחת Windows 2000, המבוסס על מפתח ציבורי.

זמן לימוד משוער: 35 דקות

חבילת אימות ערוץ מאובטח

ב-Windows 2000, חבילת אימות ערוץ מאובטח (Secure Channel Authentication Package) ממוקמת מתחת לממשק ספק תמיכת האבטחה (**S**ecurity **S**upport **P**rovider **I**nterface - SSPI), כפי שניתן לראות בתרשים 11.7.



תרשים 11.7 ארכיטקטורת שירותי אימות ב-Windows 2000.

חבילת האימות Schannel (Secure Channel) מיישמת את פרוטוקול SSL 3.0 (Secure Sockets Layer 3.0) ואת פרוטוקול TLS 1.0 (Transport Layer Security 1.0). SSL ו-TLS הם פרוטוקולי אבטחה גמישים, שיכולים להיערם בשכבות מעל לפרוטוקולי העברה אחרים. הם סומכים על טכנולוגיית אימות מבוססת-מפתח ציבורי (PK), ומשתמשים במשא ומתן מבוסס-מפתח ציבורי לגבי המפתח, כדי לחולל מפתח הצפנה ייחודי לכל שיח לקוח/שרת. הם מזוהים ביותר עם יישומים מבוססי אינטרנט ועם פרוטוקול HTTP (הידוע בכינוי HTTPS).

פרוטוקול TLS מבוסס על פרוטוקול SSL 3.0 והוא מועבר כתקן IETF (**I**nternet **E**ngineering **T**ask **F**orce). ההבדלים בין TLS 1.0 לבין SSL 3.0 אינם משמעותיים, אך הם מספיקים כדי למנוע משני תקני אבטחה אלו לעבוד במשולב. עם זאת, TLS 1.0 כולל מנגנון ניהול משא ומתן, המאפשר לו לצעוד לאחור ולהשתמש ב- SSL 3.0. לכן, לקוח התומך רק בפרוטוקול SSL 3.0, עדיין יכול לתקשר עם שרת התומך בפרוטוקול TLS 1.0.

גם פרוטוקול TLS וגם פרוטוקול SSL מספקים התקשרות נתונים מאובטחת על ידי הצפנה ופיענוח נתונים, אימות לקוח ואימות שרת אופציונלי. שניהם משמשים בדרך כלל לשליחה וקבלה של תקשורת פרטית דרך האינטרנט, תוך שימוש בקריפטוגרפיית המפתח הציבורי כאמצעי האימות.

פרוטוקול SSL/TLS מיושם על ידי ספק Schannel (כגון IIS, שרת Proxy ו-Exchange) ועל ידי יישומי לקוח העוברים באינטרנט (כגון Internet Explorer ולקוחות הדואר האלקטרוני ב- Outlook). יישומים מבקשים את שירותיהם של SSL ושל TLS באמצעות SSPI API.

יתרונותיהם של SSL ושל TLS כוללים, בין היתר, את הנקודות הבאות:

- אימות המבטיח ללקוח כי הנתונים נשלחים לשרת הנכון וכי השרת מאובטח.
- הצפנה המבטיחה שאף אחד אינו יכול לקרוא את הנתונים המוצפנים, מלבד שרת היעד.
- שלמות נתונים המבטיחה כי הנתונים לא שונו במהלך העברתם ברשת.

כרטיסים חכמים

כרטיסים חכמים (Smart Cards), שהם כרטיסים בגודל כרטיס אשראי, יכולים לשמש לאחסון המפתח הציבורי, המפתח הפרטי והאישור של המשתמש. כרטיסים חכמים הם דרך מאובטחת להגן על מפתחות המשתמש ולשלוט בהם, במקום לאחסן אותם במחשב. מפתחות המשתמש והאישור שלו נעים ממקום למקום יחד איתו. כל החישובים אשר אבטחת המידע קריטית עבורם, מבוצעים על ידי הכרטיס החכם, במקום לחשוף את המפתח הפרטי של המשתמש לעיני המחשב. בנוסף, כרטיסים חכמים מרחיבים פתרונות מבוססי תוכנה-בלבד, כגון כניסה למערכת ודואר אלקטרוני מאובטח.

כדי להשתמש בכרטיס חכם, צריך המחשב עצמו לכלול קורא כרטיס חכם. כרטיס חכם הוא התקן התואם לתקן ISO 7816 ומכיל מיקרו-מעבד מוכלל (Embeded), מעבד משנה של RSA, או מעבד קריפטוגרפי תואם, ואחסון מקומי. האחסון המקומי כולל:

- ❖ 6KB עד 24KB של זיכרון ROM עבור מערכת ההפעלה של הכרטיס החכם והיישומים שבו.
- ❖ 128 עד 512 בתים של זיכרון RAM לנתוני ריצה בזמן אמת.
- ❖ 1KB עד 16KB ברכיב EEPROM, לנתוני המשתמש.

כניסה באמצעות כרטיס חכם

Windows 2000 מציגה אפשרות כניסה למערכת באמצעות כרטיס חכם, המבוססת על מפתח ציבורי, כחלופה לסיסמה לאימות domain (Domain Authentication). אפשרות זו מסתמכת על תשתית כרטיס חכם במחשב PC תואם-קבוצות עבודה, שהוצג לראשונה לסביבת Windows NT ו- Windows 95 בחודש דצמבר של שנת 1997, ועל כרטיס חכם, המאפשר RCA עם תמיכה בספקי שירותי קריפטוגרפיה (CSP - **C**ryptographic **S**ervice **P**roviders) מסוג CryptoAPI. תהליך האימות עושה שימוש בפרוטוקול PKINIT, כדי לשלב אימות מבוסס-מפתח ציבורי (PK-Based Authentication) עם מערכת בקרת הגישה מסוג Kerberos של Windows 2000.

בעת ההפעלה מזהה המערכת אירועי הכנסת כרטיס חכם כחלופה להקשת Alt+Ctrl+Del, המשמשת כמחרוזת להפניית תשומת לב מערך האבטחה של המערכת לאתחול תהליך כניסה למערכת. המשתמש מתבקש להקליד את קוד PIN של הכרטיס החכם, השולט על הגישה לפעולות באמצעות מפתח פרטי המאוחסן בכרטיס החכם. במערכת זו, מאוחסן בכרטיס החכם גם עותק של אישור המשתמש (אשר הונפק לו על ידי ה- Enterprise CA). אופן עבודה זה מאפשר למשתמש לנוע בין מחשבים ב-Domain.

Authenticode

הגידול בשימוש ברשת האינטרנט הוביל להסתמכות גוברת והולכת על הורדת תכנים פעילים, כגון יישומים מבוססי-Windows, פקדי ActiveX ויישומוני Java. התוצאה היתה חשש מוגבר מפני תכנים אלה, מכיון שהם נטו להתרחש כ"תופעות לוואי" של תסריטי אינטרנט, מבלי שהמשתמש יהיה מודע לכך. כתגובה לחששות אלה הוציאה חברת Microsoft לאור, בשנת 1996, את טכנולוגיית החתימה הדיגיטלית Authenticode, וכבר בשנת 1997 הציגו הרחבות ניכרות של טכנולוגיה זו.

טכנולוגיית Authenticode, המהווה מאפיין אבטחה ב-Internet Explorer, מבטיחה את אמיתות ואמינות רכיבי תוכנה ברשת האינטרנט. Authenticode מוודאת שהתוכנה לא "טופלה" ומזהה את מפרסם התוכנה. המשתמש יכול להחליט, בכל מקרה לגופו, אם ברצונו להוריד את התוכן המוצע לו. הוא יעשה זאת בהתאם לניסיונו ואם הוא סומך

על מפיץ התוכנה. על ידי חתימה על הקוד שהם יוצרים, יכולים מפתחי תוכנה ליצור יחסי אימון בינם לבין המשתמשים בתוכנה שהם יוצרים.

טכנולוגיית Authenticode מאפשרת למפיצי תוכנה לחתום בחתימה דיגיטלית כל סוג של תוכן פעיל (Active Content), כולל ארכיונים מרובי קבצים. חתימות אלו יכולות לשמש לשם וידוא מפיץ התוכן ושלמותו, בזמן הורדתו למחשב הלקוח. תשתית וידוא זו היא בקנה מידה כלל עולמי של משתמשי Windows, מכיון שהיא מסתמכת על המבנה ההירררכי של CA, בו מספר CA מסחריים קטנים מנפיקים אישורים ליצרני תוכנה. לצרכי הארגון, מאפשר לך PKI של Windows 2000 להנפיק אישורי Authenticode למפתחי הבית או לקבלני משנה, ובכך לאפשר לכל העובדים לוודא את מקור ושלמות היישומים שהם מורידים.

Encrypting File System - EFS

EFS (**E**ncrypting **F**ile **S**ystem) היא הרחבה של מערכת הקבצים NTFS המספקת אבטחת נתונים מתקדמת והצפנה עבור קבצים ותיקיות. טכנולוגיית ההצפנה מבוססת על השימוש במפתחות הציבוריים ומופעלת כשירות מערכת משולב, דבר המקל על ניהולה, מקשה על תקיפתה והיא שקופה למשתמש. דבר זה יעיל במיוחד לאבטחת נתונים הניתנים לגניבה, כגון נתונים במחשבים ניידים.

בתהליך ההצפנה נעשה שימוש במפתח הציבורי של המשתמש, מה שמבטיח את פרטיות הנתונים. פיענוח הנתונים נדחה עבור כל משתמש שאין לו את המפתח הפרטי התואם. בנוסף, עבור כל קובץ מוצפן מחולל גם מפתח שחזור מיוחד. מפתח זה משמש למקרי חירום בידי מנהל מערכת מוסמך, למקרה בו עובד עוזב את החברה או שהמפתח הפרטי אובד.

הצפנה ופיענוח מתבצעים באופן שקוף למשתמש, בעת הליכי I/O. EFS אינה גורמת להפחתה משמעותית בביצועי המערכת בעת תהליך ההצפנה/פיענוח.

EFS גם תומכת בהצפנה/פיענוח של קבצים המאוחסנים ב-NTFS volumes מרוחקות, אבל ניתן להפעילה רק על נתונים מאוחסנים. למרות שקבצים מוצפנים ניתנים לייצוא, הנתונים מועברים ברשת במבנה לא מוצפן, כברירת מחדל. Windows 2000 מספקת פרוטוקולי רשת, כגון SSL, TLS ו-IPSec, להצפנת נתונים בעת שהם עוברים ברשת.

הגנת נתונים

EFS משתמשת בשילוב של המפתח הציבורי והמפתח הפרטי של המשתמש, כמו גם במפתח אקראי להצפנת קבצים (**F**ile **E**ncryption **K**ey - FEK). FEK הוא מפתח בן 128 סיביות בגרסאות המופצות בצפון אמריקה, ובן 40 סיביות בגרסאות הבינלאומיות של Windows 2000. לשם הצפנת הקבצים משתמשת Windows 2000 באלגוריתם בשם DESX (**D**ata **E**ncryption **S**tandard **X**).

שחזור נתונים

מדיניות שחזור נתונים מוצפנים (**E**ncrypted **D**ata **R**ecovery **P**olicy - EDRP) משמשת להגדרת האופן בו ניתן יהיה לשחזר נתונים, במידה והמפתח הפרטי של משתמש יאבד. במחשבים הפועלים באופן עצמאי (Stand-alone) מחוללת EDRP באופן אוטומטי, כדי להקטין את הניהוליות. מחשבים שהם חברים ב-domain, מקבלים את EDRP שלהם ממדיניות ה-domain. לשם אבטחת המידע, מוגבל השחזור לנתונים המוצפנים בלבד; אין אפשרות לשחזר את מפתחות המשתמש.

גיבוי מוצפן ושחזור

מאחר שלחברים בקבוצת המשתמשים המקומית Backup Operators אין את המפתחות הנדרשים לצורך הפיענוח, נתונים מוצפנים המשוחזרים מגיבוי, נקראים ומאוחסנים בגיבוי כמחרוזת נתונים לא ברורה.

Fault Tolerance

הצפנה ופיענוח הן פעולות רגישות, מפני שכישלון עלול לגרום לאיבוד נתונים חשובים. בשל כך, EFS מבצעת את כל הפעולות באופן אוטומטי. אם תהליך כלשהו אינו יכול להיות מושלם, הוא מבוטל מתחילתו. לדוגמה, אם מתרחשת הפסקת חשמל בדיוק באמצע תהליך הצפנה, EFS מבטלת את הפעולה בעת האתחול מחדש של המערכת, כך שהקובץ שב למצבו הקודם.

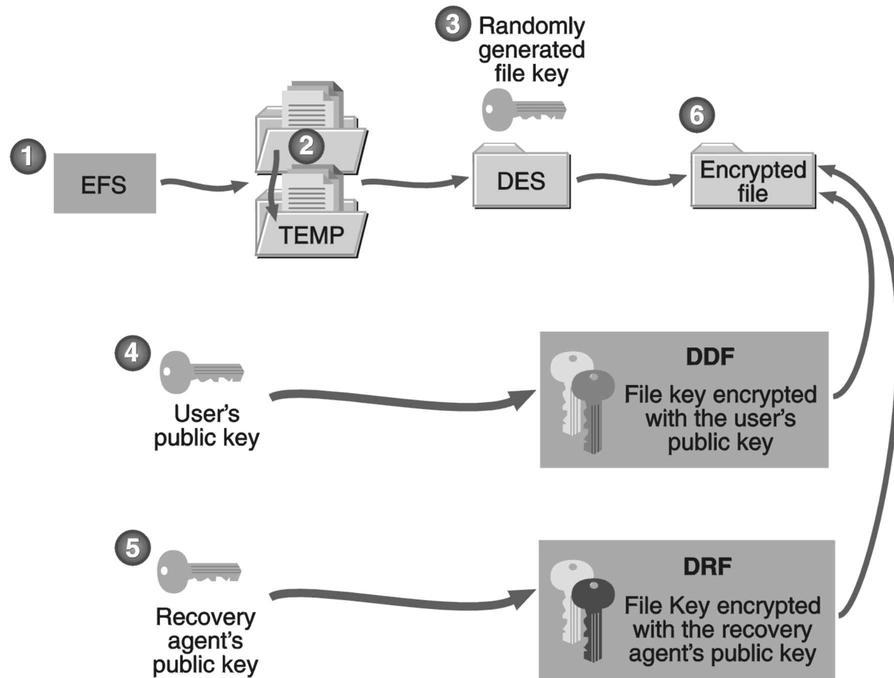
מרגע שקובץ מוצפן, תהליכי ההצפנה והפיענוח שלו הם אוטומטיים ושקופים לחלוטין למשתמש וליישומים, כאשר נעשה שימוש בקובץ. ניתן לבצע הצפנה של קובץ אחד כל פעם, או של תיקיה אחת כל פעם.

ניתן להצפין קובץ או תיקיה מתוך סייר Windows (Windows Explorer) ומשורת הפקודה (Command Prompt).

הערה אין אפשרות להשתמש גם בדחיסה **וגם** בהצפנה של NTFS על אותו קובץ.

הצפנה EFS

EFS מצפינה, מפענחת ומשחזרת קבצים. תרשים 11.8 מתאר את תהליך ההצפנה באופן כללי. הצעדים הממוספרים מפורטים בהמשך.



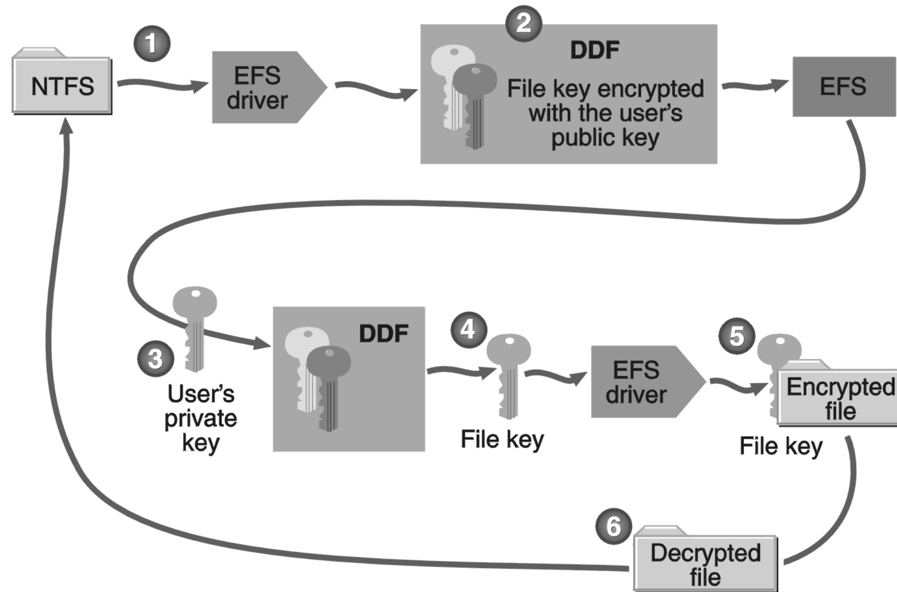
תרשים 11.8 תהליך הצפנת EFS.

כאשר משתמש מצפין קובץ ב-EFS מתרחש התהליך הבא:

1. שירות EFS פותח את הקובץ לגישה בלעדית שלו.
2. כל שטף הנתונים בקובץ מועתק לקובץ זמני.
3. מפתח קובץ מחולל באופן אקראי ומשמש להצפנת הקובץ, בהתאם לשיטת ההצפנה DES.
4. נוצר שדה פיענוח נתונים (**D**ata **D**ecryption **F**ield - DDF), המכיל את מפתח הקובץ אשר מוצפן באמצעות המפתח הציבורי של המשתמש.
5. נוצר שדה שחזור נתונים (**D**ata **R**ecovery **F**ield - DRF), המכיל את מפתח הקובץ, והפעם הוא מוצפן באמצעות המפתח הציבורי של סוכן השחזור (Recovery Agent). המפתח הציבורי של סוכן השחזור מושג מתוך מדיניות שחזור הנתונים המוצפנים (EDRP).
6. שרת EFS רושם את הנתונים המוצפנים, יחד עם DDF ו-DRF, חזרה לקובץ אחד.

פיענוח EFS

תהליך הפיענוח נעזר ב-DDF, הנוצר בעת תהליך ההצפנה, כדי לפענח קובץ. תרשים 11.9 מתאר את תהליך הפיענוח באופן כללי. הצעדים הממוספרים מפורטים בהמשך.



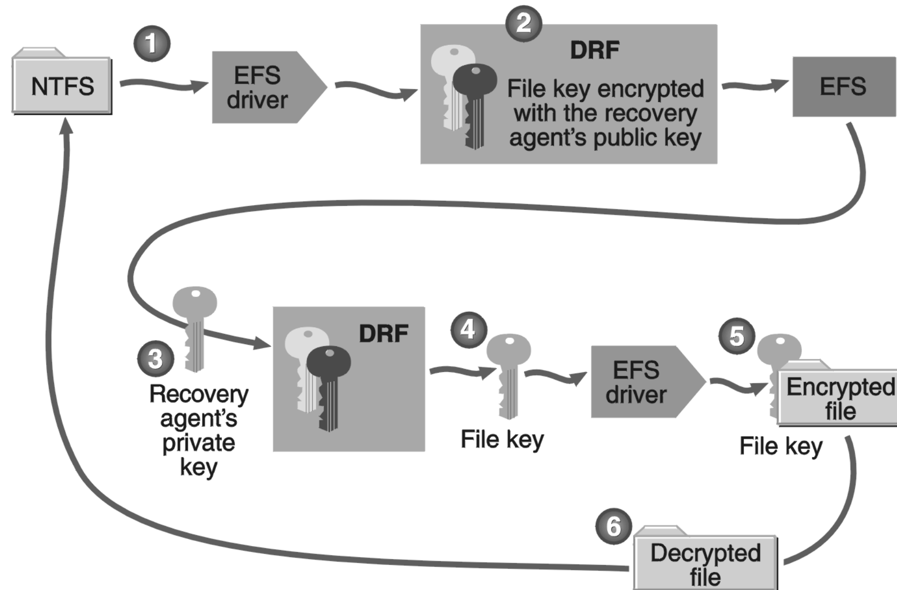
תרשים 11.9 תהליך פיענוח EFS.

כאשר קובץ מפוענח על ידי EFS מתרחשים הצעדים הבאים:

1. כאשר יישום ניגש לקובץ מוצפן, מזהה NTFS את הקובץ כמוצפן, ושולחת בקשה למנהל התקן EFS.
2. מנהל התקן EFS שולף את ה-DDF, ומעביר אותו לשירות EFS.
3. שירות EFS מפענח את ה-DDF באמצעות המפתח הפרטי של המשתמש, כדי להשיג את מפתח הקובץ.
4. שירות EFS מעביר את מפתח הקובץ חזרה למנהל התקן EFS.
5. מנהל התקן EFS נעזר במפתח הקובץ כדי לפענח את הקובץ.
6. מנהל התקן EFS מחזיר את הנתונים המפוענחים ל-NTFS, אשר מצידה משלימה את הבקשה לקובץ ושולחת את הנתונים ליישום המבקש.

שחזור EFS

שחזור EFS דומה מאוד לתהליך הפיענוח. תרשים 11.10 מתאר את תהליך השחזור באופן כללי. הצעדים הממוספרים מפורטים בהמשך.



תרשים 11.10 תהליך שחזור EFS.

כאשר קובץ משוחזר על ידי EFS מתרחשים הצעדים הבאים:

1. NTFS שולחת בקשה למנהל התקן EFS.
2. מנהל התקן EFS שולף את ה-DRF ומעביר אותו לשירות EFS.
3. שירות EFS מאושש את ה-DRF, תוך שימוש במפתח הציבורי של סוכן השחזור, כדי להשיג את מפתח הקובץ.
4. שירות EFS מעביר את מפתח הקובץ חזרה למנהל התקן EFS.
5. מנהל התקן EFS נעזר במפתח הקובץ כדי לשחזר את הקובץ.
6. מנהל התקן EFS מחזיר את הנתונים המשוחזרים ל-NTFS, אשר מצידה המשלימה את תהליך בקשת הקובץ, ושולחת את הנתונים ליישום המבקש.

Cipher - תוכנית שירות של שורת הפקודה

פקודת cipher, מאפשרת לך להצפין ולפענח קבצים ממצב DOS או מתפריט Start באפשרות Run.

תחביר הפקודה הוא כזה:

cipher [/e | /d] [/s:dir] [/a] [/I] [/f] [/q] [/h] [/k] [pathname [...]]

אם לא משתמשים במתג כלשהו, מציגה הפקודה cipher את מצב ההצפנה של התיקיה הנוכחית ושל הקבצים השמורים בה. חובה להקיש רווח בין מתגים שונים, במידה ומשתמשים בפקודה מרובת מתגים. הטבלה הבאה מתארת את המתגים האפשריים.

מתג	תיאור
/e	מצפין את התיקיות המצוינות. תיקיות מסומנות כך, שקבצים שיוספו להן בשלב מאוחר יותר - יוצפנו גם הם.
/d	מפענח את התיקיות המצוינות. תיקיות מסומנות כך, שקבצים שיוספו להן בשלב מאוחר יותר - לא יוצפנו.
/s:dir	מבצע את הפעולה המבוקשת על תיקיות בתיקיה הנבחרת ועל כל תיקיות המשנה שלהן.
/a	מבצע את הפעולה המבוקשת על קבצים בשמות המצוינים. אם לא קיימים קבצים בשמות אלה, התוכנית מתעלמת ממתג זה.
/I	ממשיך בביצוע הפעולות המבוקשות, גם לאחר שהתרחשו תקלות. כברירת מחדל, cipher עוצרת כאשר מתרחשת תקלה.
/f	מכריח את ביצוע הצפנה או פיענוח של כל האוביקטים המצוינים. כברירת מחדל, cipher מדלגת על קבצים שכבר הוצפנו או פוענחו.
/q	משחזר רק את המידע החיוני ביותר.
/h	מציג קבצים להם מאפיין של קובץ נסתר (Hidden), או קובץ מערכת (System). כברירת מחדל, קבצים אלה אינם מוצפנים או מפוענחים.
/k	יוצר אישור הצפנה חדש במחשב בו מופעלת cipher. מתג זה גורם להתעלמות מכל המתגים האחרים. לכן, השתמש במתג k/ בנפרד ממתגים אחרים.
pathname	שם הנתיב. מציין דפוס, קובץ או תיקיה. ניתן להשתמש במספר מרובה של שמות קבצים ובתווי הכללה (Wildcards).

דוגמאות

כדי להצפין את התיקיה C:\My Documents, הקלד **cipher /e "My Documents"** במחוון הפקודה C:\>.

כדי להצפין את כל הקבצים בכונן :C אשר שמם כולל את המילה test, הקלד את הפקודה **cipher /e /s *test*** במחוון הפקודה C:\>.

תרגיל 2: הגדרה ושימוש בהצפנת קבצים

בתרגיל זה תגדיר מדיניות התאוששות נתונים (Data Recovery) ב-Domain, ואז תצפין תיקיה. בצע תרגיל זה במחשב Server01.

הערה לתרגול נוסף, פתח את \Chapt11\articles\efs-wp.doc שבתקליטור המצורף לספר זה והשלם את התרגילים 2 עד 7, החל בעמוד 12.

הליך 1: הגדרת מדיניות התאוששות נתונים עבור Domain

ברירת מחדל של מדיניות התאוששות מוגדרת, כאשר ה-Domain Controller מותקן לראשונה. כתוצאה מכך, אישור המוחתם באופן עצמי, ממנה את ה-Domain Administrator כסוכן ההתאוששות. בהליך זה תוסיף את ה-Domain Administrator כסוכן ההתאוששות באופן ידני, לפני השימוש ב-EFS.

1. היכנס ל- Server01 בשם משתמש administrator ועם הסיסמה password.
2. לחץ Start, לחץ Run, ודא כי כתובת דף טופס ההרשמה לשירות האישורים (http://server01/certsrv/) מופיעה ולחץ OK. Internet Explorer ייפתח ויציג את דף ההרשמה.
3. ודא כי לחצן האפשרויות Request A Certificate נבחר, ולחץ Next. יופיע הדף Choose Request Type.
4. לחץ על לחצן האפשרויות Advanced Request, ולחץ Next.

   יופיע הדף Advanced Certificate Request.
5. ודא כי לחצן האפשרויות Submit A Certificate Request To This CA Using A Form נבחר ולחץ Next. יופיע דף הטופס Advanced Certificate Requests.
6. מתיבת הרשימה הנפתחת Certificate Template, בחר את EFS Recovery Agent.
7. לחץ על Submit. יופיע הדף Certificate Issued.
8. לחץ על הקישור Install This Certificate. יופיע הדף Certificate Installed.
9. סגור את חלון Internet Explorer.

הערה ניתן להשלים את כל הצעדים בהליך זה מתוך תוסף התוכנה Group Policy. בצעד 19 של הליך זה עליך לבחור Create במקום Add. האפשרות Create יוצרת את האישור, ואז מאפשרת לך לשייך אותו למדיניות הקבוצתית.

10. פתח את תוסף התוכנה Active Directory Users and Computers מתוך קבוצת היישומים Administrative tools.
11. הרחב את חלון Tree, ובחר בצומת microsoft.com.
12. פתח את תפריט Action, ובחר Properties.
13. תופיע תיבת הדו-שיח microsoft.com Properties.
14. בחר בכרטיסיה Group Policy, ולחץ על Edit. יופיע תוסף התוכנה Group Policy.
15. תחת הצומת Computer Configuration, הרחב את המכולה Windows Settings.
16. תחת המכולה Windows Settings, הרחב את הצומת Security Settings.
17. תחת הצומת Security Settings, הרחב את המכולה Public Key Policies.
18. תחת המכולה Public Key Policies, הרחב את המכולה Encrypted Data Recovery Agents.
19. פתח את תפריט Action, ובחר Add. יופיע האשף Add Recovery Agent.
20. לחץ Next. יופיע המסך Select Recovery Agents.
21. קרא את הכתוב במסך Select Recovery Agents, ולחץ על Browse Directory.

    תופיע תיבת הדו-שיח Find Users, Contacts, And Groups.
22. לחץ על Find Now.
23. ברשימה Users and Computers, לחץ לחיצה כפולה על Administrator.

    יופיע המסך Select Recover Agents.
24. לחץ Next. יופיע מסך האשף Completing The Adding Recovery Agent.
25. לחץ Finish. המשתמש Administrator יופיע בחלונית הפרטים של תוסף התוכנה Group Policy.
26. לחץ על הרשומה בחלונית הפרטים.
27. פתח את תפריט Action ובחר Properties. תופיע תיבת הדו-שיח Administrator Properties.

    שים לב שכל המטרות מסומנות כמאופשרות עבור אישור זה. המטרה היחידה הזמינה ברגע זה עבור אישור זה היא File Recovery.

28. לחץ OK.

29. סגור את תוסף התוכנה Group Policy. תיבת הדו-שיח microsoft.com Properties תופיע.

30. לחץ OK. יופיע תוסף התוכנה Active Directory Users and Computers.

31. פתח את תפריט View, ולחץ על Advanced Features.

32. בחלון Tree לחץ על המכולה Users.

33. בחלונית הפרטים לחץ על Administrator.

34. פתח את תפריט Action וממנו בחר Properties. תופיע תיבת הדו-שיח Administrator Properties.

35. בחר בכרטיסיה Publish Certificates. תופיע רשימת אישורי X.509 המפורסמים של משתמש זה.

שים לב כי פורסמו שני אישורים עבור חשבון המשתמש Administrator, וכי הן הונפקו על ידי המשתמש Administrator. האישור הרשום בעמודה Intended Purpose כ-File Recovery משמש להתאוששות קבצים המוצפנים ב-EFS, במידה והמפתח הפרטי אבד, או שאינו חוקי מסיבה אחרת כלשהי.

36. לחץ OK.

37. סגור את תוסף התוכנה Active Directory Users and Computers.

הליך 2: הצפנת תיקיה באמצעות EFS

בהליך זה תצפין תיקיה תוך שימוש בסייר Windows (Windows Explorer) במחשב Server01.

1. בשולחן העבודה, לחץ לחיצה כפולה על הסמל My Computer.

   יופיע החלון My Computer.

2. לחץ לחיצה כפולה על הסמל של כונן :C. מופיע חלון המציג את כונן :C.
3. לחץ לחיצה כפולה על סמל התיקיה Documents and Settings. יופיע חלון התיקיה Documents and Settings.
4. לחץ לחיצה כפולה על סמל התיקיה Administartor. יופיע חלון התיקיה Administrator.
5. לחץ על סמל התיקיה My Documents.
6. פתח את תפריט File, ובחר Properties. תיבת הדו-שיח My Documents Properties תופיע.
7. לחץ על הלחצן Advanced. תופיע תיבת הדו-שיח Advanced Attributes.
8. סמן את תיבת הסימון Encrypt Contents To Secure Data, ולחץ OK. תופיע תיבת הדו-שיח My Documents Properties.
9. לחץ OK. תופיע תיבת הדו-שיח Confirm Attribute Changes.
10. לחץ על לחצן האפשרויות Apply Changes To This Folder, Subfolders And Files.
11. לחץ OK. תופיע תיבת הדו-שיח My Documents Properties ולאחריה תופיע תיבת ההודעה Applying Attributes. כאשר התהליך מושלם, נסגרת גם תיבת הדו-שיח My Documents Properties.
12. יופיע החלון Administrator.

    שים לב שבאזור התיאור של התיקיה הנבחרת My Documents שבחלון מופיע Attributes כ- Encrypted.

13. סגור את חלון Administrator.

אבטחת IP

בפרק הקודם ניתנה סקירה כללית של IPSec, בעת הדיון בנושא פרוטוקולי תיעול. פרק זה ממשיך בדיון אודות IPSec, ומספק פרטים נוספים אודות השימוש ב-IPSec לתמיכה באבטחת המפתח הציבורי.

IPSec בסביבת Windows 2000, נועד להגן על נתונים רגישים ברשת מבוססת TCP/IP. IPSec יעיל כאשר הרשת בין שני מחשבים המתקשרים ביניהם אינה מאובטחת. הוא מספק סודיות (Confidentiality), שלמות (Integrity) ואימות (Authentication) של תנועת IP עבור כל מנה המועברת ברשת.

בעת השימוש ב-IPSec, מסכימים ביניהם שני המחשבים המתקשרים לגבי מדיניות האבטחה המשותפת הגבוהה ביותר; אז, מטפל כל אחד מהם באבטחת IP מצידו שלו. לפני שליחת נתונים דרך הרשת מצפין המחשב השולח את הנתונים, באופן שקוף לעיני המשתמש, תוך שימוש באבטחת IP (IP Security). מחשב היעד מפענח את הנתונים, גם הוא באופן שקוף לעיני המשתמש, לפני שהוא מעביר אותם לתהליך היעד. מכיון שהנתונים מועברים ומוצפנים ברמת פרוטוקול IP, לא נדרשות חבילות אבטחה שונות עבור כל פרוטוקול בחבילת הפרוטוקולים TCP/IP.

השימוש ב-IPSec להצפנת כל תנועת הנתונים ברשת IP, מבטיח כי כל תקשורת מבוססת-IP מאובטחת מפני ציתותים. כל הנתבים או המתגים שבנתיב בין המחשבים המתקשרים, יכולים להעביר את מנות IP המוצפנות הללו.

הערה מחשב Windows 2000 המוגדר לפעול עם IPSec, שולח את הנתונים למערכות הפעלה קודמות ל-Windows 2000 ללא הצפנה כלשהי. מצב זה נועד להבטיח תאימות מלאה עם גרסאות קודמות של Windows.

מדיניות IPSec

עם IPSec של Windows 2000 תוכל ליצור מדיניות המגדירות את סוג ורמת האבטחה, שיהיו בשימוש בעת התקשרות רשת.

מדיניות משא ומתן

מדיניות משא ומתן (Negotiation Policy) קובעת את שירותי האבטחה, בהם ייעשה שימוש בעת התקשרויות רשת. פרוטוקול האבטחה הנבחר למדיניות המשא ומתן, יהווה את הבסיס לשירותי האבטחה. לדוגמה, אם נבחר פרוטוקול IP Authentication Header, יסופקו שירותי שלמות, אימות ומניעת שידור חוזר, אך לא יסופק שירות הסודיות.

ניתן לקבוע מספר שיטות אבטחה לכל מדיניות משא ומתן. אם השיטה הראשונה אינה מקובלת על ידי משייך האבטחה, השירות ממשיך לנסות על פי הרשימה, עד אשר הוא

מוצא מדיניות המתאימה ליצירת השיוך. אם המשא ומתן נכשל, מתבצעת ההתקשרות ללא IPSec.

מסנני IP

מסנני IP (IP Filters) מכוונים פעולות המבוססות על יעדה של מנת IP, איזה פרוטוקול IP פעיל ועל היציאות המשויכות בהן משתמש הפרוטוקול. כל מנת IP נבדקת מול מסנן IP, ואם נמצאה התאמה, משמשים מאפייני אותה מדיניות אבטחה לשליחת ההתקשרות. מסננים צריכים להיות מוגדרים לתנועה נכנסת ולתנועה יוצאת של תעבורת רשת.

מדינויות אבטחה

מדינויות אבטחה (Security policies) משמשות להגדרת תכונות IPSec. מדינויות אלו בנויות ממדיניות משא ומתן משויכות וממסנני IP, והן משויכות למדיניות של ה-DC. מדינויות אבטחה מגדירות את סוג ורמת האבטחה, בה ייעשה שימוש בכל התקשרות IP נתונה. מדיניות אבטחת IP יכולה להיות מוקצית למדיניות ברירת המחדל של ה-Domain, מדיניות ברירת המחדל המקומית או מדיניות Domain המותאמת באופן אישי.

מחשב הנכנס ל-Domain מקבל באופן אוטומטי את המאפיינים של מדיניות ברירת המחדל המקומית ושל ה-Domain, כולל את מדיניות IPSec המוקצית למדיניות ה-Domain.

רכיבי IPSec

תהליך ההתקנה של Windows 2000 מתקין את השירותים, פרוטוקולים ומנהלי ההתקן הדרושים עבור IPSec:

- ❖ שירות סוכן מדיניות IPSec (IPSec Policy Agent service).
- ❖ פרוטוקול איגוד האבטחה של האינטרנט וניהול מפתחות (ISAKMP - **I**nternet **S**ecurity **A**ssociation and **K**ey **M**anagement **P**rotocol).
- ❖ פרוטוקול ניהול מפתחות של אוקלי (Oakley Key Management Protocol).
- ❖ מנהל התקן IPSec.

ל-ISAKMP ולפרוטוקול ניהול מפתחות של אוקלי נהוג להתייחס כאל פרוטוקול IKE - ISAKMP/Oakley.

IPSec Policy Agent Service

בעת אתחול המערכת, מושך שירות סוכן מדיניות IPSec (IPSec Policy Agent Service) מדיניות IPSec משירות Active Directory. שירות סוכן מדיניות IPSec מעביר את נתוני המדיניות למנהל התקן רשת IPSec ולפרוטוקולים ISAKMP/Oakley. שירות סוכן מדיניות IPSec אינו מאחסן מדינויות באופן מקומי; במקום זאת הוא חייב למשוך אותן ממחסן Active Directory. השירות גם מפעיל את הפרוטוקול IKE - ISAKMP/Oakley ואת מנהל התקן IPSec.

הפרוטוקולים IKE - ISAKMP/Oakley

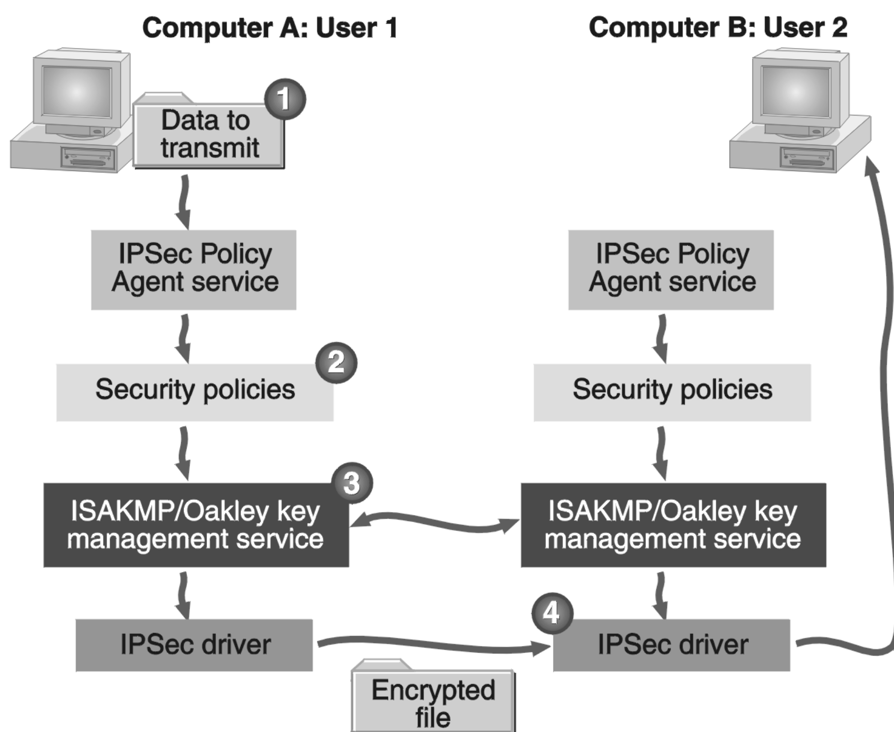
בעת השימוש בנתונים שבמדיניות IPSec, מנהלים הפרוטוקולים IKE - ISAKMP/Oakley משא ומתן ומקימים איגוד אבטחה (**S**ecurity **A**ssociation - SA) בין המחשבים. שירות Kerberos מאמת את זהותם של המחשבים המתקשרים. לבסוף, הפרוטוקולים IKE - ISAKMP/Oakley שולחים את ה-SA ונתוני מפתח למנהל התקן IPSec.

מנהל התקן IPSec

מנהל התקן IPSec (IPSec Driver) בוחן את כל מנות ה- IP, ומחפש התאמה למסנן IP. אם נמצאת התאמה, מחזיק מנהל התקן IPSec את המנות בתור, בעוד שהפרוטוקולים IKE - ISAKMP/Oakley מחוללים את ה-SA והמפתח הנדרשים לאבטח את המנה. לאחר שמנהל התקן IPSec מקבל את הנתונים מהפרוטוקולים IKE - ISAKMP/Oakley, הוא מצפין את מנות ה-IP ושולח אותן למחשב היעד.

דוגמה להתקשרות IPSec

בדוגמה זו, משתמש 1 במחשב A שולח נתונים למשתמש 2 במחשב B. אבטחת IP מיושמת בשני המחשבים. תרשים 11.11 מתאר מבט כללי של תהליך התקשרות IPSec. הצעדים הממוספרים מוסברים בהמשך.



תרשים 11.11 דוגמה לתהליך התקשרות IPSec.

ברמת המשתמש, תהליך אבטחת מנת IP הוא שקוף ופועל כך:

1. משתמש 1 מפעיל יישום המתקשר ברשת באמצעות TCP/IP, כדי לשלוח נתונים למשתמש 2. מדיניות האבטחה המוקצות למחשב A ולמחשב B קובעות את רמת האבטחה להתקשרות רשת זו.
2. שירות סוכן מדיניות IPSec מושך את המדיניות ומעביר אותן לפרוטוקולים IKE - ISAKMP/Oakley ולמנהל התקן IPSec.
3. הפרוטוקולים IKE - ISAKMP/Oakley בכל מחשב משתמשים במדיניות המשא ומתן המשויכת למדיניות האבטחה המוקצית, כדי להקים את המפתח ואת שיטת ניהול המשא ומתן המשותף, או איגוד אבטחה (SA). תוצאות המשא ומתן של מדיניות האבטחה מועברות בין שני המחשבים אל מנהל התקן IPSec, הנעזר במפתח לשם הצפנת הנתונים.
4. לבסוף, מנהל התקן IPSec שולח את הנתונים המוצפנים למחשב B. מנהל התקן IPSec שבמחשב B מפענח את הנתונים ומעביר אותם ליישום המקבל.

סיכום שיעור

Windows 2000 מרחיבה את נושא האבטחה, על ידי תמיכה במספר טכנולוגיות המבוססות על אבטחת מפתח ציבורי, כולל חבילת אימות SChannel, כרטיסים חכמים, Authenticode, מערכת הקבצים המוצפנת EFS ופרוטוקול האבטחה של האינטרנט IPSec. חבילת אימות SChannel מיישמת את SSL 3.0 ואת TLS 1.0. SSL ו-TLS הם פרוטוקולי אבטחה גמישים, שיכולים להיות מונחים בשכבות מעל פרוטוקולי תעבורה אחרים. כרטיסים חכמים הם התקנים בגודל כרטיס אשראי רגיל, שיכולים לשמש לאחסון המפתח הפרטי, המפתח הציבורי והאישור של המשתמש. כרטיס חכם הוא דרך מאובטחת לשמירה ולבקרה על מפתחות המשתמש, במקום לשמור אותם במחשב. טכנולוגיית Authenticode מאפשרת ליצרני תוכנה לחתום בחתימה דיגיטלית כל צורה של תוכן פעיל, כולל קבצי ארכיון מרובי-קבצים. חתימות אלו יכולות לשמש לאימות של המוציא לאור וגם של התוכן, ושל שלמות הנתונים אותם מוריד המשתמש. EFS היא הרחבה של מערכת הקבצים NTFS, ומספקת הגנה יעילה לנתונים והצפנת קבצים ותיקיות. טכנולוגיית ההצפנה מבוססת על השימוש במפתח הציבורי ופועלת כשירות מערכת משולב. IPSec בסביבת Windows 2000 נועד להגן על נתונים רגישים ברשת TCP/IP. IPSec יעיל כאשר הרשת בין שני מחשבים מתקשרים אינה מאובטחת. הוא מספק סודיות, שלמות ואימות תנועת IP לכל מנה.

שיעור 3: פרוטוקול Kerberos

תהליך תקני בנושא אבטחת נתונים במחשבים הוא לכלול פונקציה, הדורשת ממשתמשים להוכיח את זהותם. הצהרה זו של הזהות מושגת, כאשר המשתמש מספק את הסיסמה המתאימה לחשבון המשתמש. לדוגמה, כאשר User1 מנסה להתחבר לשרת כדי לגשת לקובץ, חייב השרת להיות בטוח כי זה באמת User1 השולח את הבקשה. בדרך כלל, מניח השרת כי זהו באמת User1, מפני שסופקה הסיסמה הנכונה בעת יצירת ההתקשרות. אבטחה הדוקה יותר מושגת באמצעות צד שלישי נסמך המוודא את זהות המשתמש. זהו עיקרון הפעולה של פרוטוקול האימות Kerberos.

לאחר שיעור זה, תוכל

- לתאר את פרוטוקול Kerberos, וכיצד הוא פועל בסביבת Windows 2000.

זמן לימוד משוער: 35 דקות

מבוא לפרוטוקול Kerberos

פרוטוקול Kerberos הוא ספק האימות שבברירת המחדל של Windows 2000, ומהווה גם את פרוטוקול האבטחה העיקרי בה. הוא מאפשר ללקוחות להשתמש בכניסה אחת לרשת לשם גישה לכל המשאבים. פרוטוקול Kerberos מוודא הן את אמיתות המשתמש והן את שלמות נתוני ה-Session. דבר זה מושג על ידי שירות Kerberos המותקן בכל Domain Controller ולקוח Kerberos המותקן בכל המחשבים הפועלים בסביבת Windows 2000.

הערה לקוח Active Directory עבור Windows 9x מאפשר למשתמשים להיכנס לרשת, תוך שימוש בפרוטוקול אימות Kerberos V5.

כאשר נעשה שימוש בפרוטוקול האימות Kerberos, מוודא ה-trusted Kerberos service בשרת את זהות המשתמש. לפני שהוא מתחבר לשרת, מבקש המשתמש כרטיס (Ticket) משירות Kerberos (השירות נקרא שירות מרכז הפצת מפתח Kerberos, או באנגלית Kerberos Key Distribution Center Service), כדי לוודא את זהות המשתמש. אז, שולח המשתמש את הכרטיס שקיבל לשרת היעד. מכיון שהשרת סומך על שירות Kerberos שיערוב לזהויות המשתמשים, מקבל השרת את הכרטיס, כהוכחה לאמיתות המשתמש.

כאשר נעשה שמוש בפרוטוקול אימות Kerberos, משתמשים כבר אינם יכולים פשוט להיכנס ולגשת למשאבים, רק על ידי הנפקת זיהוי משתמש חוקי וסיסמה תואמת. במקום לסמוך על המקור, חייב המשאב להתקשר עם שירות Kerberos, כדי לקבל כרטיס הערב למשתמש.

שירות Kerberos מתפקד כ-Trusted Third-party, כדי לחולל מפתחות session, ולהעניק כרטיסים ל-specific client/server sessions.

כרטיס המונפק על ידי שירות Kerberos מכיל את הרכיבים הבאים :

- Session Key
- שם הלקוח לו הונפק ה-Session Key
- Expiration period של הכרטיס
- שדות נתונים נוספים או הגדרות שייתכן שיידרשו

משך פקיעת תוקף הכרטיס נקבע על ידי Domain Policy. אם תוקף הכרטיס פג בעת שה-session פעיל, מתריע על כך שירות Kerberos בפני הלקוח ובפני השרת, ומתרה בהם לחדש את תוקף הכרטיס. אז, שירות Kerberos מחולל Session Key חדש וה-Session ממשיך.

מונחים בפרוטוקול Kerberos

כדי להבין טוב יותר את פרוטוקול Kerberos, עליך לסקור את המונחים הבאים, המשמשים לתיאור רכיביו השונים של הפרוטוקול.

Principal

Principal הוא שם ייחודי, הניתן למשתמש/לקוח/שרת המשתתף בהתקשרויות רשת.

Realm

Realm הוא תחום אימות (Authentication Boundary), הניתן להשוואה ל-Windows 2000 Domain. כל ארגון המבקש להפעיל שרת Kerberos, מייסד את ה-Realm שלו. Domain של Windows 2000 הוא Realm של Kerberos, אך הוא נקרא Domain, כדי לשמר את מוסכמת מתן השמות המיושמת מתקופת Windows NT.

Secret Key

Secret Key (מפתח סודי) הוא מפתח הצפנה (Encryption Key), המשותף בין לקוח או שרת לבין צד שלישי נסמך, כדי להצפין את הנתונים המיועדים להיות מועברים ביניהם. במקרה של Kerberos, הצד השלישי הנסמך הוא שירות Kerberos. במקרה של Principal, בדרך כלל מבוסס המפתח הסודי על Hash או על הצפנת סיסמת ה-Principal. מפתחות סודיים לעולם אינם מועברים ברשת; מועברים רק הנתונים המוצפנים.

Session Key

Session Key הוא מפתח הצפנה זמני, המשמש בין שני Principals, כאשר אורך חייו מוגבל לאורכו של משך התחברות (Login Session) אחד. ה-Session Key מוחלף בין השותפים המתקשרים, ולכן הוא מוכר כסוד משותף (Shared Secret). ה-Session Key נשלח תמיד מוצפן.

Authenticator

Authenticator (מאמת) הוא רשומה, המשמשת לווידוא שמקור הבקשה הוא אכן Principal. מאמת מכיל מידע, המוודא את זהות השולח ואת השעה בה נוצרה הבקשה. מידע זה מוצפן באמצעות Session Key משותף הידוע רק ל-Principals המתקשרים. בדרך כלל נשלח המאמת יחד עם כרטיס, כדי לאפשר לצד המקבל לוודא שהלקוח המיועד אכן יצר בקשה לפני זמן קצר.

KDC - Key Distribution Center

KDC (מרכז הפצת מפתח) מספק שתי פונקציות: שרת אימות (AS - **A**uthentication **S**erver) ושירות הענקת הכרטיס (**T**icket **G**ranting **S**ervice - TGS). TGS מפיץ כרטיסים ללקוחות המבקשים להתחבר לשירותים ברשת. אולם, לפני שלקוח יוכל להשתמש ב-TGS כדי להשיג כרטיסים, עליו קודם כל להשיג כרטיס מיוחד (כרטיס המעניק כרטיס, **T**icket **G**ranting **T**icket - TGT) משרת האימות.

PAC - Privilege Attribute Certificate

PAC (תעודת מאפייני זכויות יתר) היא מבנה המכיל את מזהה האבטחה של המשתמש (**S**ecurity **ID** - SID).

Tickets

בחלופת Kerberos בסיסית, יוצר הלקוח קשר עם TGS ומבקש כרטיס עבור שרת היעד, לפני שהוא מתקשר עם שרת היעד עצמו. כרטיס (Ticket) הוא רשומה המאפשרת ללקוח לאמת את עצמו בפני השרת; זוהי פשוט תעודה מאשרת, המונפקת על ידי שירות Kerberos. הכרטיס מוצפן כך, שרק שרת היעד מסוגל לפענח ולקרוא אותו. כרטיסים מכילים את זהות הלקוח המבקש, חותמת שעה, Session Key של השרת, אורך חיי הכרטיס ומידע נוסף (כגון PAC) אשר יסייע לוודא את זהות הלקוח בפני שרת היעד. כרטיסים ניתנים לשימוש חוזר לאורך תקופת תוקפם, שבדרך כלל מוגדרת למשך של 8 שעות.

TGT - Ticket Granting Tickets

שיטה אחת לשימוש ב-Kerberos היא על ידי בקשת כרטיס, עבור כל שרת יעד מחלק ה- TGS של שירות Kerberos, בכל פעם שהמשתמש מעוניין לגשת למשאב בשרת יעד כלשהו. בשימוש בשיטה זו תכיל התגובה Session Key ומידע נוסף, המוצפן באמצעות המפתח הסודי של המשתמש. שיטה זו גורמת לחשיפה ברשת של רכיבים מתוך המפתח הסודי של המשתמש, בכל פעם שמבוצעת בקשה חדשה לכרטיס.

בסביבת Windows 2000 מגן Kerberos על המפתח הסודי על ידי אימות המשתמש קודם כל ואז בקשת TGT. כרטיס המעניק כרטיס (**T**icket **G**ranting **T**icket - TGT) זוהי בקשה לכרטיס ו-Session Key אקראי, אשר ישמש במשולב לחלק ה- TGS של שירות Kerberos. לאחר קבלת הכרטיס, יכול המשתמש לתקשר עם השירות בכל זמן;

הכרטיס המבוקש אינו מגיע משרת אימות (AS), אלא משירות הענקת הכרטיס (TGS). התשובה מוצפנת לא באמצעות המפתח הסודי של המשתמש, אלא באמצעות ה-Session Key, אותו סיפק שרת האימות לשימוש עם שירות הענקת הכרטיס (TGS).

מאפיינים בפרוטוקול Kerberos

לפרוטוקול Kerberos יש מספר יתרונות על מערכות אימות המוכרות מסוג Challenge/Respond (דרישה להזדהות/תגובה).

תקן פתוח מפותח

יישום פרוטוקול Kerberos בסביבת Windows 2000 נסמך על מסמכי RFC 1510 ו- RFC 1964. הוא יכול לפעול במשולב עם יישומים אחרים של Kerberos אשר תואמים לאותם מסמכי RFC. בשל כך, לקוחות Kerberos בפלטפורמות אחרות, כגון UNIX, יכולים להיות מאומתים על ידי Windows 2000. אבל, במקרים מסוימים ערכים תלויי-יישום לא יתקיימו, או שלא יהיו זמינים. בהעדרם של נתונים נדרשים, מנסה שירות Kerberos של Windows 2000 להתאים את שם ה-Principal שבכרטיס לחשבון משתמש של Windows 2000, או לחשבון ברירת המחדל, שנוצר במיוחד למטרה זו.

אימות התחברות מהיר יותר

בעת השימוש בפרוטוקול Kerberos, אין השרתים צריכים לבצע אימות עובר (Pass-Through Authentication). שרת Windows 2000 יכול לוודא את נתוני המשתמש באמצעות כרטיס המסופק על ידי המשתמש עצמו, מבלי שיידרש לבצע שאילתה בשירות Kerberos. זאת, מכיון שהלקוח כבר קיבל כרטיס מ-Domain Controller, והשרת יכול להשתמש בו כדי לבנות את אסימון הגישה (Access token) של הלקוח. מאחר שהשרת אמור לבצע פחות עבודה כאשר נוצרת ההתחברות, הוא יכול בקלות רבה יותר להכיל מספר גדול יותר של בקשות התחברות.

אימות הדדי

פרוטוקול Kerberos מבצע אימות הדדי (Mutual Authentication) הן עבור הלקוח והן עבור השרת. פרוטוקול האימות NTLM של Windows מבצע רק אימות לקוח, והוא יוצא מנקודת הנחה שניתן לבטוח בכל השרתים. הוא אינו מוודא את זהות השרת אליו מתחבר הלקוח. ההנחה שניתן לסמוך על כל השרתים כבר אינה קיימת. אימות הדדי הן של הלקוח והן של השרת היא בסיס חשוב לאבטחת רשתות תקשורת נתונים.

האצלת סמכויות אימות

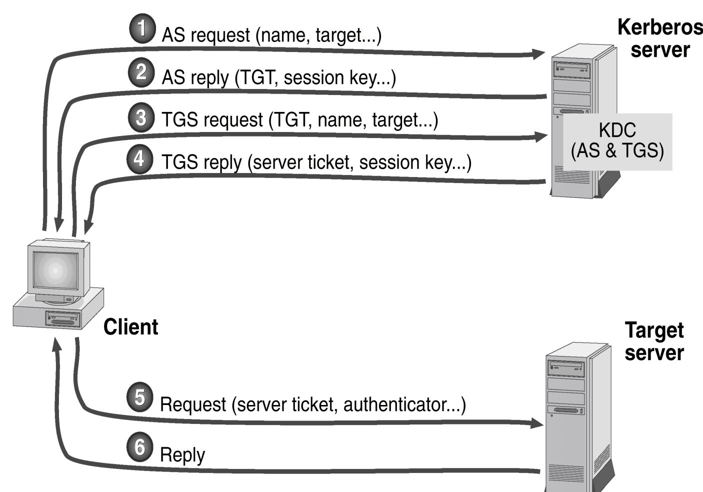
האצלת סמכויות אימות (Delegation Of Authentication) מאפשרת למשתמש להתחבר לשרת יישומים, אשר מצידו יכול להתחבר לשרת נוסף אחד, או יותר, בשמו של הלקוח, תוך שימוש בנתוני הלקוח.

יחסי אמון משורשרים

יחסי אמון משורשרים (Transitive Trusts) הם כאשר נתוני אימות המונפקים על ידי שירות Kerberos אחד, יהיו מקובלים על ידי כל שירותי Kerberos בתוך ה-Domain.

תהליך אימות Kerberos

תהליך האימות של Kerberos כולל את מחשב הלקוח, שנושא ונותן לגבי שינויים בין שרת היעד וה-KDC. תרשים 11.12 מתאר מבט כללי של תהליך האימות. הצעדים הממוספרים מתוארים בהמשך.



תרשים 11.12 תהליך האימות של Kerberos.

תהליך האימות של Kerberos פועל כך:

1. הלקוח שולח בקשת AS ראשונית לחלק שרת האימות (AS) של שירות Kerberos. ה-AS כולל את שם Principal של הלקוח ואת שם Principal של שרת היעד, אליו הוא מבקש כרטיס.

2. שירות Kerberos מחולל תגובת AS ושולח אותה אל הלקוח. התגובה מכילה:

❖ TGT לחלק ה-TGS של שירות Kerberos. ה-TGT מוצפן באמצעות המפתח הסודי של TGS. ה-TGT מכיל את ה-SID של המשתמש. על ידי הצפנת ה-TGT באמצעות המפתח הסודי של TGS, לא יכול הלקוח לשנות את מאפייני ה-SID.

❖ Session Key להחלפה עם חלק ה-TGS של שירות Kerberos. ה-Session Key מוצפן באמצעות המפתח הסודי של המשתמש. המפתח הסודי של הלקוח הוא חישוב (Computation), המתבצע על-פי סיסמת המשתמש. הוא דומה ל-Session Key המשמש לדרישה להזדהות/תגובה (Challenge/Response) של NTLM. ההצפנה כאן מקשה על גניבת ה-Session Key.

3. הלקוח מחולל ושולח בקשת TGS, המכילה את שמות ה-Principal של הלקוח ושל שרת היעד, את ה-Realms ואת ה-TGT המזהה את הלקוח.

4. חלק ה-TGS של שירות Kerberos מחולל ושולח תגובת TGS ללקוח. תגובה זו מכילה כרטיס לשרת היעד. הכרטיס מוצפן באמצעות המפתח הסודי של השרת. המפתח הסודי של השרת הוא חישוב של הסיסמה, המחולל כאשר השרת מצטרף ל-Domain. התגובה כוללת גם מידע נוסף, כולל Session Key.

5. הלקוח מחלץ את ה-Session Key עבור שרת היעד ומחולל בקשה לשרת. בקשה זו מכילה את שרת היעד, ומאמת המוצפן באמצעות ה-Session Key. הלקוח שולח בקשה זו לשרת היעד, תוך שימוש בנתיב העברה קיים.

6. שרת היעד מפענח את הכרטיס באמצעות המפתח הסודי שלו, כדי להשיג את ה-Session Key. אז, משתמש השרת ב-Session Key, כדי לפענח את המאמת, ולוודא את זהות הלקוח. אם הלקוח ביקש אימות הדדי, מחולל שרת היעד תגובה, המוצפנת באמצעות ה-Session Key, ושולח אותה ללקוח. אימות הדדי לא רק שמאמת את הלקוח בפני שרת היעד, אלא הוא גם מאמת את שרת היעד בפני הלקוח.

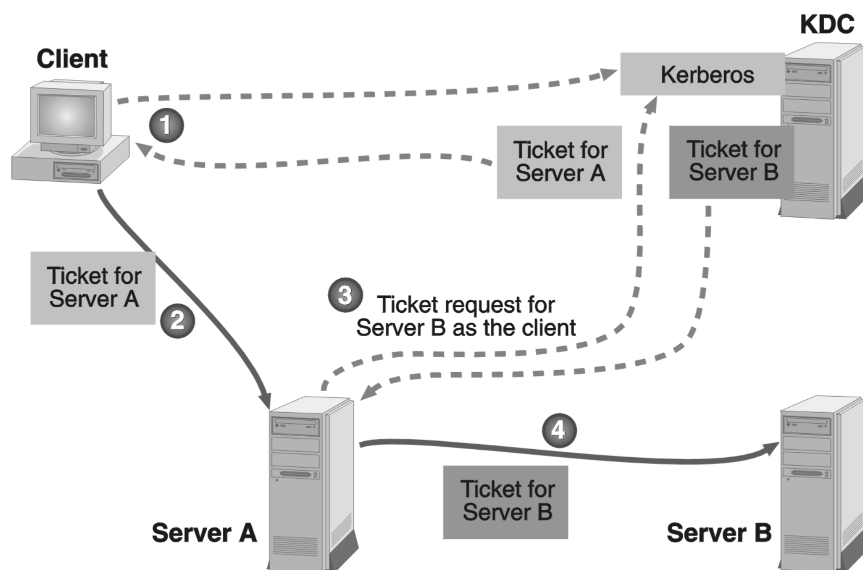
הערה חלופות AS ו-TGS עם שירות Kerberos פועלות באמצעות פרוטוקול צרורות נתוני משתמש (**U**ser **D**atagram **P**rotocol - UDP) ביציאה (Port) 88. החלופות בין הלקוח ושרת היעד תלויות בפרוטוקול המשמש בין שני ה-Principals.

האצלת סמכויות Kerberos

מדי פעם מתגלה הצורך ששרת יישומים יתחבר לשרת אחר, בשמו של הלקוח. כפי שהדבר בהתחזות (Impersonation), האצלת סמכות נועדה להבטיח, כי הרשאות אבטחה תואמות מיושמות כנגד בקשתו של שרת היישומים.

פרוטוקול האימות Kerberos תומך בהאצלת סמכויות אימות. בסוג זה של אימות נעשה שימוש כאשר פעילות הלקוח מערבת מספר שרתים. במקרה כגון זה, כל אחד מהשרתים המוודאים משיג כרטיס אחר, ומאמת את הכרטיס עבור השרת המבקש בשמו של הלקוח. אין הגבלה על מספר השרתים הרציפים (Consecutive) אשר יכולים להאציל את סמכויות האימות. דבר זה שונה מהתחזות, בכך שהשרת מבצע גישה למשאבים מרוחקים בשמו של הלקוח, במקום למשאבים מקומיים.

תרשים 11.13 מתאר בכלליות את תהליך האצלת הסמכויות של Kerberos. הצעדים הממוספרים מתוארים בהמשך.



תרשים 11.13 תהליך האצלת הסמכויות של Kerberos.

הצעדים הבאים מתארים את התהליך המתרחש בעת גישה למשאבים, המצויים בשני שרתים שונים:

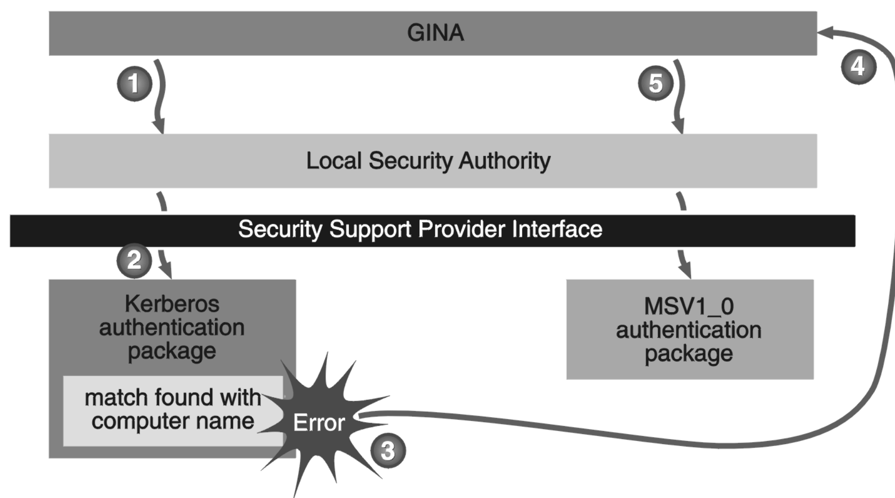
1. הלקוח מבקש ומקבל משירות Kerberos כרטיס לשרת היעד Server A.
2. הלקוח שולח את הכרטיס ישירות ל- Server A.
3. Server A מתחזה ללקוח, ושולח לשירות Kerberos בקשה לקבלת כרטיס לשרת היעד Server B. שירות Kerberos מגיב עם כרטיס המאפשר ללקוח גישה ל- Server B.
4. אז יכול Server A לשלוח את הכרטיס ל- Server B ולגשת אליו בתור הלקוח.

תהליכי כניסה של Kerberos

הוספת Kerberos כחבילת אימות לסביבת Windows 2000 משפיעה על צדדים שונים בתהליך הכניסה למערכת (Logon). אולם, חלקו של תהליך הכניסה למערכת, המופעל לפני שחבילת האימות נכנסת לפעולה, נשאר ב-Windows 2000 ללא שינוי.

כניסה אינטראקטיבית מקומית

כאשר מתבצע תהליך כניסה אינטראקטיבי מקומי, נכנס המשתמש למערכת באמצעות חשבון משתמש הקיים במחשב המקומי (Local User Account), ולא Domain User Account. תרשים 11.14 סוקר תהליך כניסה אינטראקטיבי מקומי בסביבת Windows 2000. הצעדים הממוספרים מתוארים בהמשך.



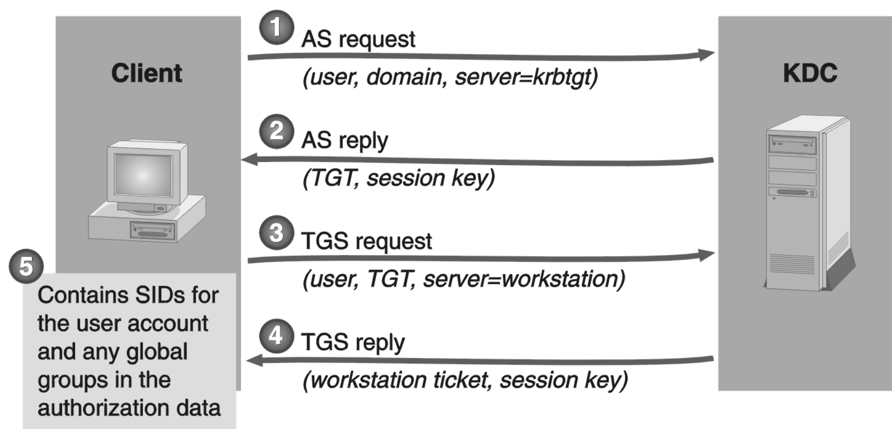
תרשים 11.14 תהליך כניסה אינטראקטיבי מקומי.

במקרה של חשבונות משתמשים מקומיים, מתרחשים ב-Windows 2000 הצעדים הבאים:

1. כאשר ספריית הקישור הדינמית **G**raphical **I**dentification and **A**uthentication (GINA) DLL מקבלת בקשת כניסה למערכת, היא מעבירה אותה אל סמכות האבטחה המקומית (Local Security Authority - LSA). בקשה זו מגדירה את Kerberos כחבילת האימות בה יש להשתמש, מפני שהיא חבילת ברירת המחדל של Windows 2000.
2. ה-LSA מעבד את הבקשה, ושולח אותה לחבילת האימות של Kerberos.
3. כאשר Kerberos מקבל את בקשת הכניסה למערכת, הוא מגיב בשגיאה, מפני שנעשה בו שימוש רק לצורך אימות כניסות של Domain Users Accounts, לא של חשבונות משתמשים מקומיים (Local Users).
4. ה-LSA מקבל את השגיאה ומחזיר שגיאה ל-GINA.
5. GINA מעבירה פעם נוספת את בקשת הכניסה ל-LSA, אך הפעם היא מציינת בשדה חבילת האימות את MSV1_0 כחבילה המבוקשת. אז מתבצע תהליך הכניסה למערכת, כפי שהוא היה מתבצע בסביבת Windows NT 4.0.

כניסה אינטראקטיבית ל-domain

החילופין (Exchange) המתבצעים כאשר משתמש נכנס ל- Windows 2000 עם Domain User Account, דומים לחילופין הבסיסיים של Kerberos. תרשים 11.15 מתאר בכלליות תהליך כניסה זה. הצעדים הממוספרים מתוארים בהמשך.



תרשים 11.15 תהליך כניסה אינטראקטיבי ל-Domain.

תהליך כניסה אינטראקטיבי ל-Domain מתרחש כך :

1. כאשר בקשת הכניסה מגיעה אל ה-LSA הוא מעביר את הבקשה לחבילת אימות Kerberos. הלקוח שולח בקשת AS ראשונית לשירות Kerberos, המספק לו שם משתמש ו-Domain Name. זוהי בקשה לאימות ול-TGT. הבקשה מתבצעת תוך שימוש בשם ה-Principal שהוא krbtgt@<domain_name>, כאשר domain_name הוא שם ה-Domain בו ממוקם חשבון המשתמש. ה-DC הראשון ב-Domain מחולל באופן אוטומטי את החשבון krbtgt@<domain_name>.
2. שירות Kerberos מחולל תגובת AS, המכילה TGT (מוצפן באמצעות המפתח הסודי של Kerberos) ו-Session Key עבור חילופי TGS (מוצפן באמצעות המפתח הסודי של המשתמש). תגובה זו נשלחת חזרה ללקוח. חלק נתוני ההרשאה של ה-TGT מכיל את ה-SID עבור חשבון המשתמש ו-SID נוספים, עבור כל קבוצה גלובלית אליה שייך המשתמש. ה-SID מוחזרים ל-LSA, כדי שייכללו באסימון הגישה של המשתמש. ה-SID מועתקים על ידי שירות Kerberos מה-TGT לכרטיסים רציפים המושגים משירות Kerberos.
3. הלקוח מחולל ושולח בקשה ל-TGS, המכילה את שם Principal של הלקוח ואת ה-Realm, ה-TGT לזיהוי הלקוח ואת שם תחנת העבודה המקומית כשרת היעד. דבר זה מתבצע, כדי לבקש גישה למחשב המקומי עבור המשתמש.
4. שירות Kerberos מחולל ושולח תגובת TGS. תגובה זו מכילה כרטיס עבור תחנת העבודה ומידע נוסף, הכולל את ה-Session Key (המוצפן באמצעות ה-Session Key של TGT). בנוסף נכללים בחלק נתוני ההרשאות SID, עבור חשבון המשתמש ועבור כל הקבוצות הגלובליות, המועתקות על ידי שירות Kerberos מה-TGT המקורי.
5. חבילת האימות של Kerberos מחזירה את רשימת ה-SID ל-LSA.

שירותי Windows 2000 משתמשים ב-SSPI (**S**ecurity **S**upport **P**rovider **I**nterface) של מצב ליבה (Kernel Mode), כדי לבצע אימות. במקום לתקשר ישירות עם חבילת האימות Kerberos, שני השירותים מבצעים גישה ל-Kerberos, באמצעות חבילת אימות המובנית בתוך ה-LSA. חבילת אימות זו נקראת חבילת משא ומתן (Negotiate Package).

בעת אתחול המערכת, הן שירות השרת והן שירות תחנת העבודה מאתחלים את הממשק שלהם עם חבילת המשא ומתן של LSA, תוך שימוש ב-SSPI. בעת תהליך זה, משיג שירות השרת Credential Handle עבור נתוני ברירת המחדל שלו.

התקשרות הרשת מתבצעת בשני קטעים : משא ומתן בין פרוטוקולים והגדרת Session. לפני שהמשתמש יוכל להקים Session עם השרת, חייבים מחשב הלקוח והשרת להסכים על פרוטוקול האבטחה בו ייעשה שימוש, כדי לקבוע באיזו גירסה של אבטחה תומכים שניהם. לאחר שהלקוח אומת וקיבל את הכרטיס שלו, הוא יכול להקים Session עם השרת.

תמיכת מפתח ציבורי של Kerberos

Windows 2000 מרחיבה את הפונקציונליות של Kerberos, כדי לאפשר לו לתקשר עם שירותי Active Directory. Windows 2000 כוללת הרחבות עבור פרוטוקול האימות Kerberos V5, המאפשרות תמיכה באימות מבוסס מפתח ציבורי. ההרחבה למפתח הציבורי מאפשרת ללקוחות לבקש TGT ראשוני, תוך שימוש במפתח פרטי. שירות Kerberos מוודא בקשה מעין זו, תוך שימוש במפתח הציבורי של המשתמש, אותו הוא משיג מנתוני X.509 שלו, המפורסמים במחסן Active Directory. כדי להשיג כרטיס, חייבים נתוני X.509 של המשתמש להיות מאוחסנים באובייקט המשתמש. אם שירות Kerberos מוצא את הנתונים, הוא מנפיק כרטיס ללקוח, ומכאן והלאה ממשיך תהליך Kerberos רגיל. זה מחליף את המפתח הסודי הידוע רק ל-Principal ול-KDC. כרטיסים חכמים, לדוגמה, עושים שימוש בהרחבה עבור מפתחות ציבוריים המסופקת על ידי Kerberos.

סיכום שיעור

Kerberos הוא ספק האימות, המהווה את ברירת המחדל בסביבת Windows 2000, ופרוטוקול האבטחה העיקרי. כדי להבין את פרוטוקול Kerberos טוב יותר, עליך להכיר את המונחים השכיחים הקשורים בו, כולל Principal, Realm, מפתח סודי, Session Key, מאמת, KDC, AS, TGS, PAC, כרטיס ו-TGT. תהליך האימות של Kerberos כולל את מחשב הלקוח הנושא ונותן חלופות (Exchanges) בין שרת היעד וה-KDC. פרוטוקול האימות Kerberos תומך בהאצלת סמכויות אימות. כאשר מתרחשת כניסה אינטראקטיבית מקומית למערכת, נכנס המשתמש באמצעות חשבון משתמש המאוחסן במחשב המקומי, ולא באמצעות Domain User Account. החליפין המתרחש בעת כניסת המשתמש ל-Windows 2000, באמצעות Domain User Account, דומה לבסיס החליפין של Kerberos. שירותי Windows 2000 משתמשים ב- Kernel Mode SSPI כדי לבצע אימות. בנוסף, Windows 2000 מרחיבה את פונקציונליות Kerberos, כדי לאפשר לו לתקשר עם שירותי Active Directory. Windows 2000 כוללת הרחבות עבור פרוטוקול האימות Kerberos V5, כדי לתמוך באימות מבוסס מפתח ציבורי.

שיעור 4: כלי הגדרה לניהול אבטחה

Windows 2000 כוללת מערך כלים להגדרה ולניהול אבטחה אשר נועדו להפחית את העלויות המשויכות להגדרות אבטחה, ניתוח ואבחון רשתות Windows 2000. כלים אלה הם תוספי התוכנה (Snap-ins) של MMC (**M**icrosoft **M**anagement **C**onsole), המאפשרים לך לקבוע את הגדרות האבטחה של Windows 2000, ולבצע פעולות ניתוח תקופתיות של המערכת, כדי להבטיח שהתצורה נשארת תקינה, או כדי לבצע שינויים הנדרשים עם הזמן. הגדרות אבטחה כוללות מדיניות אבטחה (מדיניות חשבון ומדיניות מקומית), בקרת גישה (שירותים, קבצים ורישום המערכת - Registry), יומני אירועים, חברויות בקבוצות (קבוצות מוגבלות), מדיניות אבטחת IPSec ומדיניות מפתח ציבורי. כלי הגדרת תצורת האבטחה מונים שלושה תוספי תוכנה: Security Configuration and Analysis, Security Templates ו- Group Policy.

לאחר שיעור זה, תוכל

- להבין כיצד כלי הגדרת האבטחה משמשים להגדרת אפשרויות האבטחה, ולניתוח ואבחון מערכת האבטחה ברשת Windows 2000 שלך.

זמן לימוד משוער: 30 דקות

תוסף התוכנה Security Configuration and Analysis

תוסף התוכנה Security Configuration and Analysis מאפשר לך להגדיר ולנתח את אבטחת המערכת המקומית.

הגדרת אבטחה

תוסף התוכנה Security Configuration and Analysis יכול לשמש גם להגדרת אבטחת המערכת המקומית ישירות. ניתן לייבא תבניות אבטחה שנוצרו באמצעות תוסף התוכנה Security Templates, ואז להחיל אותן על אובייקט המדיניות הקבוצתית (**G**roup **P**olicy **O**bject - GPO) עבור המחשב המקומי. דבר זה מגדיר באופן מיידי את מערך האבטחה על פי הרמות המוגדרות בתבנית.

ניתוח אבטחה

מצבם של מערכת ההפעלה ושל היישומים במערכת הוא דבר דינמי. למשל, יכול להיות שיימצא הצורך לשנות באופן זמני את רמות האבטחה, כדי לאפשר פיתרון מיידי של בעיה ניהולית כלשהי, או של בעיית רשת; ייתכנו מקרים בהם לא ניתן יהיה

להשיב את השינויים למצבם הקודם. זה אומר שהמחשב עשוי שלא לעמוד בתנאי האבטחה הנהוגים בארגון.

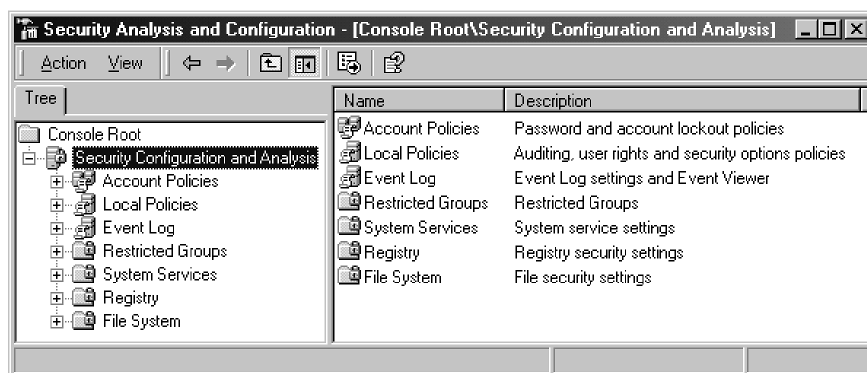
אבחון וניתוח תקופתי על בסיס קבוע מאפשר למנהל המערכת לעקוב ולהבטיח רמת אבטחה נאותה בכל מחשב, כחלק מתוכנית ניהול הסיכונים. אבחון הוא תהליך מפורט מאוד. מידע אודות כל היבטי המערכת הקשורים לאבטחה מסופק בתוצאות. דבר זה מאפשר למנהל המערכת להתאים את רמות האבטחה, וחשוב אף מזה, לאתר בעיות/תקלות אבטחה, העשויות להתרחש במערכת עם הזמן.

תוסף התוכנה Security Configuration and Analysis מאפשר סקירה חטופה של תוצאות ניתוח האבטחה. לצד הגדרות המערכת הנוכחיות מוצגות גם המלצות, וסמלים נוספים משמשים להארת אזורים, בהם ההגדרות הנוכחיות אינן תואמות את רמת האבטחה המוצעת. תוסף התוכנה גם מאפשר לך לפתור חוסרי התאמה המתגלים בניתוח המערכת.

אם יש צורך בניתוח מקיף של מספר רב של מחשבים, כפי שהדבר בתשתית מבוססת-domain, תוכל להיעזר בתוכנית שירות של שורת הפקודה Secedit כדי לבצע ניתוח באצווה. למרות שניתן להשתמש בכלי Secedit לביצוע הניתוח עצמו, כדי לצפות בתוצאות יש להשתמש בתוסף התוכנה Security Configuration and Analysis. למידע נוסף אודות תוכנית השירות Secedit פנה למערכת העזרה של Windows 2000 Server.

השימוש בתוסף התוכנה Security Configuration and Analysis

תוסף התוכנה Security Configuration and Analysis (תרשים 11.16) סוקר ומנתח את הגדרות האבטחה במערכת שלך, וממליץ על השינויים הנדרשים בה. מנהל המערכת יכול להיעזר בתוסף תוכנה, כדי להתאים את מדיניות האבטחה ולאתר בעיות/תקלות אבטחה המתרחשות בה.



תרשים 11.16 תוסף התוכנה Security Configuration and Analysis.

תוסף התוכנה Security Configuration and Analysis מאפשר לך לבצע מיגוון משימות :

- ❖ קביעת מסד נתונים לעבודה
- ❖ ייבוא תבנית אבטחה
- ❖ ניתוח אבטחת המערכת
- ❖ סקירת תוצאות ניתוח אבטחה
- ❖ הגדרת אבטחת המערכת
- ❖ עריכת תצורת האבטחה הבסיסית
- ❖ ייצוא תבנית אבטחה

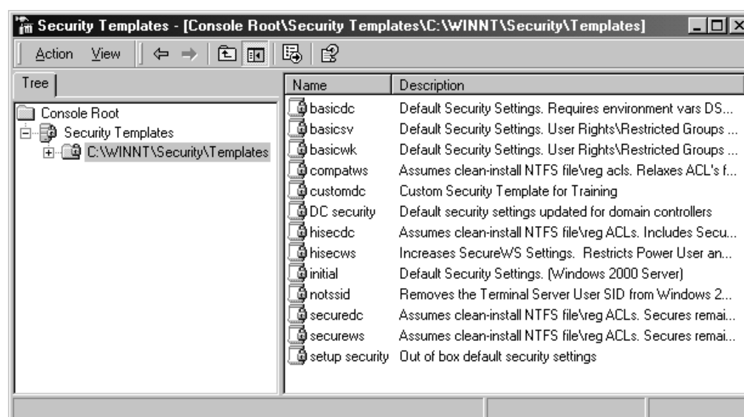
לפרטים כיצד לבצע כל אחת מהפעולות הללו, פנה למערכת העזרה של Windows 2000.

תוסף התוכנה Security Templates

תבנית אבטחה (Security Template) היא מצגת פיסית של תצורת האבטחה ; זהו קובץ בו ניתן לאחסן קבוצות של הגדרות אבטחה. Windows 2000 כוללת מספר תבניות אבטחה, כל אחת מהן מבוססת על תפקידו של המחשב. רמת התבניות נעה, החל ב-Domain Client בעל דרישות אבטחה נמוכות, ועד ל-DCs, להם דרישות אבטחה מחמירות מאוד. ניתן להשתמש בתבניות כפי שהן מגיעות במערכת ההפעלה, לשנות אותן, או להשתמש בהן כבסיס ליצירת תבניות אבטחה, המותאמות באופן מיוחד לאופי הארגון.

השימוש בתוסף התוכנה Security Templates

תוסף התוכנה Security Templates (תרשים 11.17) הוא כלי ליצירה ולהחלה של תבניות אבטחה במחשב אחד, או יותר.



תרשים 11.17 תוסף התוכנה Security Templates.

תבנית אבטחה היא מצגת של קובץ פיסי המכיל הגדרות תצורת אבטחה, אותן ניתן להחיל על מחשב מקומי, או לייבא לאובייקט מדיניות קבוצתית (GPO - **G**roup **P**olicy **O**bject) שבשירותי Active Directory. כאשר אתה מייבא תבנית אבטחה ל-GPO, מעבדת המדיניות הקבוצתית את התבנית, ויוצרת את השינויים הנדרשים לחברים באותו GPO. אלה יכולים להיות מחשבים או משתמשים.

תוסף התוכנה Security Templates מאפשר לך לבצע מיגוון משימות:

- התאמה אישית של תבנית אבטחה מוגדרת מראש
- הגדרת תבנית אבטחה
- מחיקת תבנית אבטחה
- ריענון רשימת תבניות האבטחה
- הגדרת תיאור עבור תבנית אבטחה

תרגיל 3: יצירה ושימוש בתוסף התוכנה Security Analysis and Configuration

בתרגיל זה תיצור תוסף תוכנה מותאם אישית, שיכיל את תוסף התוכנה Security Analysis and Configuration ואת תוסף התוכנה Security Templates. אז, תתאים תבנית ותפתח מסד נתונים חדש, תוך שימוש בתבנית המותאמת אישית. אחר כך תנתח את הגדרות האבטחה של Server01 מול התבנית, ותחיל את תצורת התבנית להגדרות האבטחה של Server01. בצע את התרגיל במחשב Server01.

הליך 1: יצירת תוסף התוכנה Security Analysis and Configuration

בהליך זה תפעיל את MMC, ותוסיף את תוסף התוכנה Security Analysis and Configuration. גירסה 1.2 של MMC הנכללת ב-Windows 2000 מאפשרת לך להוסיף מספר תוספי תוכנה ל-Console קיים. לשם בהירות הפעולה, תיצור console חדש, במקום להוסיף ל-console קיים המפעיל תוספי תוכנה אחרים.

1. היכנס ל-Server01 בשם משתמש Administrator ועם הסיסמה password.
2. לחץ Start ולאחר מכן לחץ Run. תופיע תיבת הדו-שיח Run.
3. בתיבת הטקסט Open הקלד **mmc**, ולחץ OK. ייפתח חלון console ריק וניתן לו שם ברירת המחדל Console1.
4. פתח את תפריט Console ובחר Add/Remove Snap-in. תופיע תיבת הדו-שיח Add/Remove Snap-in.

5. לחץ Add. יופיע החלון Add Standalone Snap-in.
6. גלול כלפי מטה, לחץ על Security Configuration And Analysis ולחץ Add.
7. לחץ Close. תופיע תיבת הדו-שיח Add/Remove Snap-in.
8. לחץ OK.
9. פתח את תפריט Console ולחץ Save. תופיע תיבת הדו-שיח Save As.
10. בתיבת הטקסט File Name הקלד **Security** ולחץ Save.

הליך 2: הוספה והגדרה של אבטחה, תוך שימוש בתוסף התוכנה Security Templates ב-Security console

לפני שתנתח את Server01 ותחיל עליו הגדרות אבטחה חדשות, עליך להתקין את תוסף התוכנה Security Templates ב-Security console שיצרת.

1. פתח את תפריט Console ובחר Add/Remove Snap-in. תופיע תיבת הדו-שיח Add/Remove Snap-in.
2. לחץ Add. יופיע החלון Add Standalone Snap-in.
3. גלול כלפי מטה, לחץ על Security Templates ולחץ Add.
4. לחץ Close. תופיע תיבת הדו-שיח Add/Remove Snap-in.
5. לחץ OK.
6. פתח את תפריט Console ולחץ Save.
7. הרחב את הצומת Security Templates והרחב את התיקיה C:\WINNT\Security\Templates. כל התבניות המוגדרות יופיעו בחלונית הפרטים של MMC Console.
8. הרחב את securedc. זוהי תבנית אבטחה אינקרימנטלית (incremental, מצטברת), בה משתמשים בדרך כלל לאחר שהוחלה תבנית האבטחה הבסיסית. למטרת תרגיל זה תבנית זו מספקת.
9. הרחב את הצומת Account Policies ולחץ על Password Policy. בחלונית הפרטים יופיעו הגדרות מדיניות הסיסמה הנוכחיות.
10. בחלונית הפרטים לחץ לחיצה כפולה על Minimum Password Length. תופיע תיבת הדו-שיח Template Security Policy Settings.

11. בתיבה Password Must Be At Least שנה את הערך ל-5 תווים ולחץ OK.
12. בחלון Tree לחץ על securedc.
13. פתח את תפריט Action ולחץ Save As. תופיע תיבת הדו-שיח Save As.
14. בתיבת הטקסט File Name הקלד **customdc** ולחץ Save.
15. בחלון Tree לחץ על customdc.
16. פתח את תפריט Action, ובחר Set Description. תופיע התיבה Security Template Description.
17. בתיבה Description הקלד **Custom Security Template for Training**, ולחץ OK.
18. בחלון Tree לחץ על התיקיה C:\WINNT\Security\Templates. שים לב שלתבנית customdc נוסף כעת גם תיאור.
19. קרא את תיאוריהן של התבניות האחרות, כדי ללמוד להכיר את התבניות הכלולות במערכת ההפעלה Windows 2000 Server.

הליך 3: יצירת מסד נתוני אבטחה חדש

בהליך זה תיצור מסד נתוני אבטחה חדש.

1. בחלון Tree לחץ על Security Configuration And Analysis, וקרא את הכתוב בחלונית הפרטים.
2. פתח את תפריט Action ובחר Open Database. תיבת הדו-שיח Open Database תופיע.
3. בתיבת הטקסט File Name הקלד **training** ולחץ Open. תופיע תיבת הדו-שיח Import Template.
4. לחץ על customdc.inf, ולחץ Open. זוהי התבנית המותאמת אישית שיצרת קודם.

הליך 4: ניתוח הגדרות האבטחה הנוכחיות

בהליך זה תנתח את ההגדרות הנוכחיות של Server01, כנגד התבנית המותאמת שיצרת בהליך 2.

1. בחלון Tree, ודא כי נבחר הצומת Security Configuration And Analysis.
2. פתח את תפריט Action, ובחר Analyze Computer Now.

   תופיע תיבת הדו-שיח Perform Analysis ובה מוצג הנתיב ושם יומן השגיאות כ- C:\Documents and Settings\Administrator\Local Settings\Temp\training.log.

3. לחץ OK.

   בעוד ההיבטים השונים של האבטחה ב-Server01 מנותחים כנגד התבנית, תופיע תיבת הדו-שיח Analyzing System Security.

4. כאשר הניתוח מסתיים, הרחב את הצומת Security Configuration And Analysis.
5. הרחב את הצומת Account Policies, ולחץ על הצומת Password Policy.

   בחלונית הפרטים יופיעו הגדרות התבנית והגדרות המחשב עבור כל מדיניות. חוסרי התאמה מצויינים בעיגול אדום ובמרכזו הסימן X בלבן. התאמה בין הגדרות התבנית והגדרות המחשב מצויינת על ידי עיגול לבן ובו סימן ✓ ירוק. אם לא מופיע סימן כלשהו, משמעות הדבר היא שלא מוגדרת מדיניות אבטחה כגון זו בתבנית.

6. בחלון Tree לחץ על הצומת Security Configuration And Analysis.
7. פתח את תפריט Action, ובחר Configure Computer Now. תופיע תיבת הדו-שיח Configure System.
8. לחץ OK.
9. פתח את תפריט Action, ובחר Analyze Computer Now. תופיע תיבת הדו-שיח Perform Analysis.
10. לחץ OK.
11. סקור את הגדרות המדיניות, כדי לוודא שתוכן העמודה Database Setting זהה לתוכן העמודה Computer Setting.
12. סגור את חלון תוסף התוכנה Security. תיבת ההודעה Microsoft Management Console תופיע.
13. לחץ Yes.
14. אם מופיע חלון Save Security Templates, לחץ Yes.

תוסף התוכנה Group policy

הגדרות אבטחה מגדירות את אופי האבטחה במערכת. תוך שימוש ב-GPO (אובייקט מדיניות קבוצה) בשירותי Active Directory, יכול מנהל המערכת להחיל באופן מרוכז רמות אבטחה הנדרשות להגנה על המערכת הארגונית.

בעת קביעת הגדרות עבור GPO המכיל מספר מחשבים, חובה להתחשב בארגון ובאופי הפונקציונלי של האתר, ה-Domain או ה-OU. לדוגמה, רמות האבטחה הנדרשות עבור יחידה ארגונית המכילה מחשבים במחלקת המכירות, תהיינה שונות במהותן מרמות האבטחה הנדרשות עבור יחידה ארגונית המכילה את מחשבי מחלקת כספים.

תוסף התוכנה Group policy מאפשר לך להגדיר אבטחה באופן מרוכז במחסן Active Directory. תיקיית Security Settings נמצאת בצומת Computer Configuration ובצומת User Configuration. הגדרות האבטחה מאפשרות למנהלי מדיניות קבוצתית לקבוע מדיניות המגבילה את גישת המשתמש לקבצים ותיקיות, לקבוע כמה סיסמאות שגויות יכול המשתמש להקליד לפני שהוא ננעל, ולשלוט בזכויות המשתמש, כגון איזה משתמש יוכל להיכנס לשרת ה-Domain. למידע נוסף אודות השימוש בתוסף התוכנה Group Policy וכיצד לנהל מדיניות קבוצתית, קרא בפרק 7 את שיעור 4, "ניהול מדיניות קבוצה".

סיכום שיעור

Windows 2000 מספקת מיגוון כלי הגדרת תצורה, המאפשרים לך לקבוע את הגדרות האבטחה של Windows 2000, ולבצע ניתוח תקופתי של המערכת, כדי להבטיח שהתצורה נשארה שלמה, או כדי לבצע את השינויים הנדרשים עם הזמן. תוסף התוכנה Security Configuration and Analysis מאפשר לך להגדיר ולנתח את האבטחה במערכת מקומית. הוא סוקר ומנתח את הגדרות האבטחה של המערכת, וממליץ על שינויים שראוי לבצע. תוסף התוכנה Security Templates מאפשר לך ליצור ולהחיל תבניות אבטחה במחשב אחד או יותר. תוסף התוכנה Group Policy מאפשר לך להגדיר את האבטחה באופן מרוכז במחסן Active Directory.

שיעור 5:
Windows 2000 Auditing

בשיעור זה תלמד אודות מעקב (Auditing) בסביבת Windows 2000, שהיא הכלי לתחזוקת אבטחת הרשת. מעקב מאפשרת לך לעקוב אחר פעילויות של משתמש ואירועים המתרחשים במרחבי המערכת. בנוסף, תלמד אודות מדיניות מעקב ומה עליך לקחת בחשבון, לפני שתגדיר מדיניות כזו. תלמד גם כיצד להגדיר מעקב לגבי משאבים וכיצד לתחזק יומני אבטחה.

לאחר שיעור זה, תוכל

- לתכנן אסטרטגיית מעקב ולקבוע אחר איזה אירועים יש לעקוב.
- להגדיר ביקורת על אובייקטים ב-Active Directory וקבצים, תיקיות ומדפסות.
- להיעזר ביומן אירועי המערכת (Event Viewer) לצפייה באירועים ולאיתורם.

זמן לימוד משוער: 75 דקות

סקירה כללית של מעקב בסביבת Windows 2000

Windows 2000 Auditing היא תהליך של מעקב אחר פעילויות המשתמש ופעילויות מערכת ההפעלה (Called Events, אירועים נקראים) במחשב. באמצעות המעקב, תוכל לציין ש-Windows 2000 תרשום רשומה של אירוע ליומן אירועי האבטחה (Security Log). ביומן אירועי האבטחה מופיעות רשומות עבור ניסיונות כניסה חוקיים ולא חוקיים למערכת ואירועים הקשורים בפתיחה, יצירה או מחיקה של קבצים או אובייקטים אחרים. רשומת מעקב ביומן אירועי האבטחה מכילה את המידע הבא:

- הפעולה שבוצעה.
- המשתמש שביצע את הפעולה.
- הצלחה או כישלון האירוע, והאירוע שהתרחש בעקבות כך.

השימוש במדיניות מעקב

מדיניות מעקב מגדירה את סוגי אירועי האבטחה, אותן תרשום Windows 2000 ליומן האבטחה בכל מחשב. יומן אירועי האבטחה מאפשר לך לעקוב אחר אירועים שאתה מגדיר.

Windows 2000 רושמת אירועים ליומן אירועי האבטחה, במחשב בו מתרחש האירוע. לדוגמה, אתה יכול להגדיר מעקב, כך שבכל פעם שמישהו מנסה להיכנס ל-Domain, תוך שימוש ב-Domain User Account והניסיון נכשל, תרשום Windows 2000 אירוע ליומן אירועי האבטחה שב-DC, במקום במחשב בו התבצע ניסיון הכניסה. זאת מפני שה-DC הוא זה אליו נעשה הניסיון להיכנס והוא זה שלא הצליח לאמת את ניסיון הכניסה.

תוכל להגדיר את מדיניות המעקב למחשב, כך שתבצע את הפעולות הבאות:

- לעקוב אחר הצלחה או כישלון אירועים, כגון ניסיונות כניסה של משתמשים, ניסיון של משתמש מסוים לקרוא קובץ מסוים, שינויים לחשבון משתמש או לחברות בקבוצות ושינויים להגדרות האבטחה שלך.
- לחסל או להקטין את הסיכון שבשימוש לא מורשה במשאבים.

תוכל להיעזר ב- Event Viewer כדי לצפות באירועים אותם רשמה Windows 2000 ביומן אירועי האבטחה. תוכל גם לשמור קבצי יומן בארכיון כדי לבצע מעקב אחר מגמות, לדוגמה, כדי לקבוע את השימוש במדפסות או קבצים או כדי לוודא ניסיונות לא מורשים לשימוש במשאבים.

תכנון מדיניות מעקב

כאשר אתה מתכנן מדיניות מעקב, עליך לקבוע באיזה מחשבים אתה מעוניין להגדיר אותה. כברירת מחדל, המעקב אינו פעיל. כשאתה מחליט איזה מחשבים יבוקרו, עליך גם לתכנן אחר מה לעקוב בכל מחשב. Windows 2000 רושמת אירועי מעקב בכל מחשב בנפרד.

סוגי האירועים שנין לעקוב אחריהם:

- גישה לקבצים או תיקיות.
- כניסה ויציאה של משתמשים.
- כיבוי והפעלה מחדש של שרתי Windows 2000.
- שינוי חשבון משתמש וקבוצות.
- ניסיונות לשינוי אובייקטים של Active Directory.

לאחר שקבעת את סוגי האירועים אחריהם תעקוב, עליך לקבוע האם יש לעקוב אחר הצלחת האירוע ו/או את כישלונו. מעקב אחר אירועים מוצלחים יכול לומר לך כמה פעמים מבצעים משתמשים או שירותים גישה מוצלחת לקבצים מסוימים, מדפסות או אובייקטים אחרים. תוכל להיעזר במידע זה לתכנון משאבים. מעקב אחר אירועים שנכשלו יכול להתריע בפניך לגבי אפשרויות של פרצות באבטחה. לדוגמה, אם מצאת מספר רב של ניסיונות כניסה כושלים למערכת, שבוצעו כולם באמצעות אותו חשבון משתמש, ובמיוחד אם ניסיונות אלו נעשו שלא בשעות העבודה הרגילות, ייתכן שאדם שאינו מורשה מנסה לפרוץ למערכת שלך.

שקול את הנקודות הבאות לקביעת מדיניות המעקב שלך:

- החלט האם ברצונך לעקוב אחר מגמות שימוש במערכת. אם כן, תכנן לשמור קבצי יומן בארכיונים. שמירת קבצי יומן אלה תאפשר לך לצפות באופן בו משתנה השימוש במערכות במשך הזמן, וכך יתאפשר לך לתכנן את משאבי מערכת, לפני שאלו יהפכו לבעיה.
- סקור יומני אירועי אבטחה לעיתים קרובות. עליך לקבוע לעצמך זמן קבוע ולסקור את היומנים באופן קבוע ורציף, מפני שהגדרת מדיניות מעקב כשלעצמה, אינה מתריעה בפניך אודות פרצות באבטחה.
- הגדר את מדיניות המעקב, כך שתהיה יעילה וקלה לניהול. עקוב תמיד נתונים חשובים ורגישים. עקוב רק את האירועים שיכולים לספק לך מידע חיוני אודות סביבת הרשת שלך. הדבר יקטין את השימוש במשאבי מערכת, ויקל על מציאת מידע חיוני. מעקב על סוגים רבים מדי של אירועים, תגרום לתקורה גבוהה מדי של Windows 2000.
- עקוב אחר גישה למשאבים של הקבוצה Everyone, ולא רק של הקבוצה Users. הדבר יבטיח לך שאתה עוקב אחר כל מי שיכול להתחבר לרשת, לא רק משתמשים, להם יצרת Domain User Account.

יישום מדיניות מעקב

מעקב (Auditing) היא כלי חשוב למעקב אחר אירועים המתרחשים במחשבים בארגון שלך. כדי ליישם מעקב, עליך להתחשב בדרישות המעקב ולקבוע מדיניות למעקב. לאחר שתגדיר מדיניות מעקב במחשב, תוכל ליישם מעקב על קבצים, תיקיות, מדפסות ואובייקטים של Active Directory.

הגדרת מעקב

תוכל ליישם מדיניות מעקב, בהתבסס על תפקידו של המחשב ברשת Windows 2000. מעקב מוגדר באופן שונה, עבור הסוגים הבאים של מחשבים הפועלים בסביבת Windows 2000:

- לשרתים המוגדרים כ- Member Server או כ- Stand-alone Server (שרתים חברים או שרתים עצמאיים), או מחשבים הפועלים בסביבת Windows 2000 Professional, מדיניות מעקב מוגדרת לכל מחשב בנפרד. לדוגמה, כדי לעקוב אחר גישות משתמשים לקובץ במחשב Member Server, עליך להגדיר את מדיניות המעקב במחשב זה.
- במקרה של DCs, מדיניות מעקב מוגדרת עבור כל ה-DCs שב-Domain. כדי לעקוב אחר אירועים המתרחשים ב-DCs, כגון שינויים לאובייקטים של Active Directory, עליך להגדיר מדיניות קבוצתית ל-Domain, שמיושמת בכל ה-DCs.

הערה סוגי האירועים אותם אתה יכול לעקוב אחריהם ב-DC, זהים לאלה שאתה יכול לעקוב אחריהם במחשב שאינו DC. ההליך זהה גם הוא, אך אתה משתמש במדיניות קבוצתית עבור ה-Domain, כדי לשלוט במעקב DCs.

דרישות למעקב

הדרישות להגדרה ולניהול מעקב הן:

- צריכה להיות לך הרשאה Manage Auditing And Security Log במחשב בו אתה מעוניין להגדיר מדיניות מעקב, או שבו אתה מעוניין לצפות בקבצי יומן של המעקב. Windows 2000 מעניקה כברירת מחדל הרשאות אלו לקבוצת המשתמשים Administrators.
- הקבצים והתיקיות לגביהם מופעל המעקב, חייבים להיות ב-NTFS volume.

הגדרת מעקב אוביקטיים

הגדרת מעקב אוביקטיים היא תהליך דו-שלבי:

- **הגדרת מדיניות המעקב** – מדיניות המעקב מאפשרת את המעקב אחר אובייקטים, אך אינה מפעילה מעקב על אובייקטים מסוימים.
- **אפשור מעקב לגבי משאבים מסוימים** – אתה מזהה את האירועים המסוימים למעקב אחר קבצים, תיקיות ואובייקטים של Active Directory. Windows 2000 תעקוב ותרשום את האירועים המסוימים הללו.

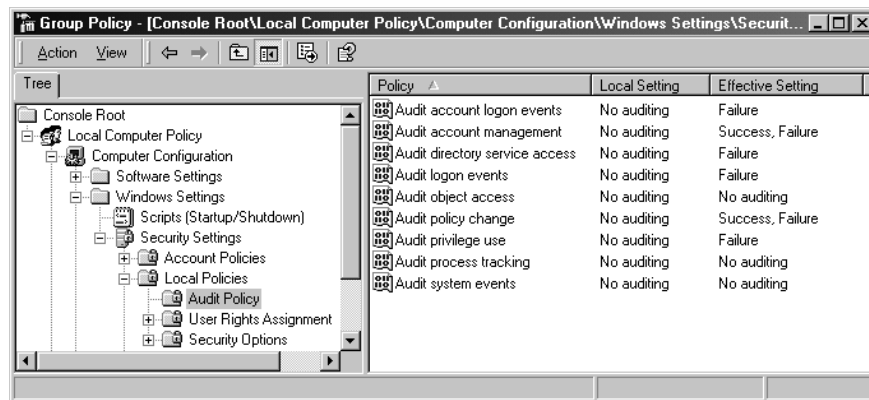
הגדרת מדיניות מעקב

הצעד הראשון ביישום מדיניות מעקב הוא בחירת סוגי האירועים אחריהם תבצע מעקב Windows 2000. עבור כל אירוע אחריו אתה יכול לעקוב, מציינות הגדרות התצורה האם לעקוב אחר ניסיון מוצלח או כושל. באפשרותך לקבוע מדיניות מעקב באמצעות תוסף התוכנה Group Policy.

הטבלה שלהלן מתארת את סוגי האירועים הניתנים לבקרה על ידי Windows 2000.

אירוע	תיאור
Account logon events	DC מקבל בקשה לאישור חשבון משתמש.
Account Management	מנהל (Administrator) יוצר, משנה או מוחק חשבון משתמש או קבוצה. שמו של חשבון משתמש שונה, החשבון בוטל או הופעל, או שנקבעה סיסמה או שונתה.
Directory service access	משתמש קיבל גישה לאובייקט של Active Directory. עליך להגדיר מעקב על אובייקטים מסוימים של Active Directory כדי לרשום סוג זה של אירוע.
Logon events	משתמש נכנס או יצא מהמערכת, או שמשתמש יצר או ביטל חיבור רשת למחשב (התחבר למשהו דרך הרשת).
Object access	משתמש ביצע גישה לקובץ, תיקיה או מדפסת. עליך לציין על איזה קבצים, תיקיות ומדפסות יש לבצע מעקב. גישה לשירות ספריית הרשת הוא מעקב על גישת משתמש לאובייקט Active Directory מסוים. גישה לאובייקט הוא מעקב על גישת משתמש לקבצים, תיקיות ומדפסות.
Policy change	בוצע שינוי באפשרויות האבטחה של המשתמש, זכויות המשתמש או מדיניות המעקב.
Privilege use	המשתמש עשה שימוש בזכות, כגון שינוי שעון המערכת (אין הדבר כולל זכויות המשויכות לתהליך הכניסה או היציאה מהמערכת).
Process tracking	תוכנית ביצעה פעולה. מידע זה יעיל, בדרך כלל, רק עבור מתכנתים המעוניינים לעקוב אחר פרטים בהפעלת התוכנית.
System	משתמש אתחל את המחשב או כיבה אותו, או שהתרחש אירוע שהשפיע על אבטחת Windows 2000, או על יומן אירועי האבטחה (לדוגמה, יומן אירועי המעקב מלא ו-Windows 2000 מוחקת רשומות).

כדי להגדיר מדיניות מעקב במחשב שאינו DC, צור MMC consloe מותאם, והוסף לו את תוסף התוכנה Group Policy. בחלון Tree בחר Group Policy מהצומת Computer Configuration, כפי שמוצג בתרשים 11.18. ה-Console מציג את הגדרות מדיניות המעקב הנוכחית בחלונית הפרטים.



תרשים 11.18 תוסף התוכנה Group Policy כאשר התיקיה Audit Policy נבחרת.

שינויים שתבצע במדיניות המעקב במחשב שלך ייכנסו לתוקף, כאשר מתרחש אחד מהאירועים הבאים:

- ❖ אתה יוזם הפצת מדיניות על ידי הקלדה בשורת הפקודה: **secedit /RefreshPolicy machine_policy** והקשה על Enter.
- ❖ אתה מאתחל את המחשב שלך. Windows 2000 מחילה שינויים שאתה מבצע במדיניות המעקב, בפעם הבאה בה יופעל המחשב.
- ❖ מתרחשת הפצת מדיניות. הפצת מדיניות (Policy Propagation) הוא תהליך המחיל הגדרות מדיניות, כולל הגדרות מדיניות מעקב, במחשב שלך. הפצת מדיניות אוטומטית מתבצעת בפרקי זמן קבועים הניתנים להגדרה. ברירת המחדל להתרחשות הפצת מדיניות אוטומטית היא כל 8 שעות.

מעקב גישה לקבצים ולתיקיות

אם פרצות באבטחה הן נושא חשוב בארגון שלך, תוכל להגדיר מעקב עבור קבצים ותיקיות במחיצות NTFS. כדי לעקוב אחר גישת משתמשים לקבצים ותיקיות, עליך קודם כל לאפשר את מדיניות מעקב גישה לאובייקטים (Audit Object Access Policy), אשר כוללת קבצים ותיקיות.

לאחר שהגדרת את מדיניות המעקב שלך לגישה לאובייקטים, אתה מאפשר ביצוע מעקב לגבי קבצים מסוימים ותיקיות, ומציין את סוגי גישה, על פי משתמש או על פי קבוצה, אחריה יש לעקוב. כדי לאפשר ביצוע מעקב לקובץ מסוים או תיקיה, פתח את תיבת הדו-שיח Properties של אותו קובץ/תיקיה, בחר בכרטיסיה Security ולחץ Advanced. בחר בכרטיסיה Auditing, והגדר את נושא המעקב לקובץ/תיקיה הנבחרים.

מעקב גישה לאובייקטים של Active Directory

כדי לבצע מעקב על גישה לאובייקטים של Active Directory עליך להגדיר מדיניות מעקב ואז לקבוע ביצוע מעקב לאובייקטים מסוימים, כגון משתמשים, מחשבים, OUs או קבוצות, על ידי ציון איזה סוגי גישה, וציון מעקב הגישה של איזה משתמשים.

כדי לאפשר ביצוע מעקב של גישה לאובייקטים של Active Directory, אפשר את מדיניות מעקב הגישה לשירותי ספריית הרשת (Audit Directory Services Access) בתוסף התוכנה Group Policy.

כדי לאפשר ביצוע מעקב לאובייקטים מסוימים ב-Active Directory, פתח את תוסף התוכנה Active Directory Users and Computers, ומתפריט View בחר Advanced Features. פתח את תיבת הדו-שיח Properties של האובייקט אחריו אתה מעוניין לעקוב. בכרטיסיה Security לחץ Advanced. בחר בכרטיסיה Auditing, והגדר מעקב עבור האובייקט.

הערה מעקב גישה למדפסות נדרש לעיתים כבסיס לגביית תשלום בעבור השימוש במדפסת.

מעקב גישה למדפסות

ניתן לבצע מעקב גישה למדפסות, כדי לעקוב אחר מדפסות רגישות. כדי לעקוב אחר הגישה למדפסות, אפשר את המדיניות Audit Object Access, אשר כוללת מדפסות. אז, אפשר ביצוע מעקב עבור מדפסות מסוימות, וקבע אחר איזה סוגי גישה יש לעקוב, וגישה מצידם של איזה משתמשים יש לעקוב. לאחר שבחרת את המדפסת, אתה פועל באותה הדרך כפי שפעלת להגדרת מעקב על קבצים ותיקיות.

כדי להגדיר מעקב על מדפסת, פתח את תיבת הדו-שיח Properties של המדפסת אחריה יש לעקוב. בחר בכרטיסיה Security, לחץ על Advanced, בחר בכרטיסיה Auditing והגדר אפשרויות מעקב למדפסת.

השימוש ב- Event Viewer

תוכל להיעזר ב- Event Viewer, כדי לבצע מיגוון משימות, כולל צפייה ביומני הביקורות הנוצרים כתוצאה מהגדרת מדיניות מעקב ואירועי מעקב. תוכל להשתמש ב- Event Viewer גם כדי לצפות בתוכן קבצי יומן אירועי האבטחה, ולאתר אירוע מסוים בתוך קבצים אלה.

יומני Windows 2000

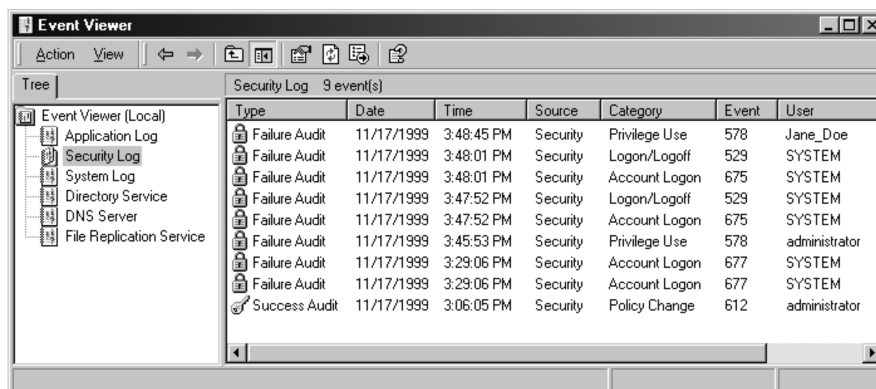
תוכל להיעזר ב-Event Viewer, כדי לצפות במידע הנכלל בקבצי היומן של Windows 2000. כברירת מחדל קיימים שלושה יומנים זמינים לתצוגה ב-Event Viewer. יומנים אלה מתוארים בטבלה שלהלן.

יומן	תיאור
Application Log	מכיל שגיאות, אזהרות, או מידע, שתוכניות, כגון תוכנת בסיס נתונים או דואר אלקטרוני, מחוללות. מפתח התוכנה קובע מראש איזה אירועים יירשמו ליומן.
Security Log	מכיל מידע אודות הצלחה ו/או כישלון פעולות מעקב. האירועים אותם רושמת Windows 2000, הם תוצאה של מדיניות המעקב שלך.
System Log	מכיל שגיאות, אזהרות ומידע ש-Windows 2000 מחוללת. Windows 2000 מגדירה מראש איזה אירועים יירשמו.

הערה אם מותקנים שירותים נוספים, הם עשויים להוסיף יומן אירועים משלהם. לדוגמה, שירות DNS (**D**omain **N**ame **S**ystem) רושם אירועי DNS לקובץ יומן DNS Server.

צפייה ביומן האבטחה

יומן האבטחה (Security Log) מכיל מידע אודות אירועים, המנוטרים על ידי מדיניות מעקב, כגון ניסיונות כניסה מוצלחים או כושלים למערכת. ניתן לצפות ביומן האבטחה בתוסף התוכנה Event Viewer, כפי שנראה בתרשים 11.19.



תרשים 11.19 תוסף התוכנה Event Viewer, ובו Security Log נבחר.

בחלונית הפרטים מציג Event Viewer רשימה של רשומות יומן ותקציר מידע לגבי כל פריט.

אירועים מוצלחים מוצגים עם סמל מפתח, ואילו אירועים כושלים מוצגים עם סמל מנעול. מידע חשוב אחר כולל את התאריך והשעה בה התרחש האירוע, קטגוריית האירוע, והמשתמש שגרם לאירוע. הקטגוריה מציינת את סוג האירוע, כגון גישה לאובייקט, ניהול חשבון, גישה לשירותי ספריית הרשת או אירועי כניסה למערכת.

Windows 2000 רושמת אירועי יומן אבטחה במחשב בו הם מתרחשים. תוכל לצפות באירועים אלה, כל עוד יש בידך הרשאות זכויות יתר ניהוליות במחשב בו התרחשו האירועים. כדי לצפות ביומן אירועי אבטחה במחשב מרוחק, הצבע עם Event Viewer למחשב המרוחק, כשאתה מתקין את תוסף התוכנה הזה ב-MMC Console.

איתור וסינון אירועים

כשאתה מפעיל את Event Viewer לראשונה הוא מציג באופן אוטומטי את כל האירועים שנרשמו ביומן הנבחר. כדי לשנות את מה שמופיע בתצוגת היומן, אתה יכול לאתר אירועים מסוימים על ידי הפעלת הפקודה Filter. אתה יכול גם לחפש אחר אירועים מסוימים באמצעות הפקודה Find. כדי לסנן או לאתר אירועים, הפעל את Event Viewer, פתח את תפריט View ובחר Filter או Find.

ניהול יומני מעקב

ניתן לעקוב אחר מגמות ב- Windows 2000, על ידי שמירת קבצי יומני אירועים והשוואת יומנים מתקופות שונות. צפייה במגמות תסייע לך לקבוע שימוש במשאבים ולתכנן את צמיחת הארגון. אם הבעיה היא שימוש לא מורשה במשאבים, תוכל להיעזר ביומנים כדי לקבוע דפוס שימוש. Windows 2000 מאפשרת שליטה בגודל קבצי היומן, והגדרת הפעולה שתתבצע על ידי מערכת ההפעלה, במידה והיומן מתמלא.

תוכל להגדיר את מאפייני כל יומן מעקב באופן עצמאי. כדי לקבוע הגדרות עבור יומן, בחר בו ב- Event Viewer, ואז הצג את תיבת הדו-שיח Properties שלו.

היעזר בתיבת הדו-שיח Properties עבור כל סוג יומן מעקב כדי לשלוט בגודלו של כל קובץ, אשר יכול להיות 64KB ועד 4,194,240KB (שהם 4GB). גודל ברירת המחדל של קובץ יומן הוא 512KB. בנוסף, באמצעות תיבת הדו-שיח Properties של קובץ היומן תוכל לבחור בפעולה שתבצע מערכת ההפעלה כאשר היומן מתמלא.

טיפ השתמש בתוסף התוכנה Security Configuration And Analysis, כדי לקבוע הגדרות עבור Event Viewer.

שמירת יומנים

שמירה ארכיונית של קבצי יומן מאפשרת לך לשמר היסטוריה של אירועים הקשורים בנושא האבטחה. לחברות רבות יש מדיניות של שמירת קבצי יומן למשך תקופה מוגדרת, לצורך מעקב אחר מידע הקשור בנושאי אבטחה לאורך זמן. אם אתה מעוניין לשמור את קובץ היומן, נקה ממנו את כל האירועים, או פתח קובץ יומן, בחר את היומן מתוך חלון Tree בצופה האירועים, ובחר באפשרות הרצויה לך תפריט Action.

סיכום שיעור

ביצוע מעקב ב-Windows 2000 הוא תהליך של מעקב אחר פעילויות המשתמש ופעילויות מערכת ההפעלה, אירועים נקראים במחשב עצמו. באמצעות המעקב תוכל להגדיר ש-Windows 2000 תרשום רשומה עבור אירוע ביומן אירועי האבטחה. מדיניות מעקב קובעת את סוג אירועי האבטחה שמערכת ההפעלה תרשום ביומן אירועי האבטחה בכל מחשב. יומן האבטחה מאפשר לך לעקוב אחר אירועים שאתה מגדיר. כשאתה מתכנן מדיניות מעקב, עליך לקבוע באיזה מחשב תגדיר את המעקב. כשאתה קובע איזה מחשב ינוטר בעת המעקב, עליך גם לתכנן אחר מה לעקוב בכל מחשב. כדי ליישם מעקב, עליך להחליט לגבי דרישות המעקב, ולקבוע מדיניות מעקב. לאחר שתגדיר מדיניות מעקב במחשב, תוכל ליישם מעקב על קבצים, תיקיות, מדפסות ואובייקטים של Active Directory. תוכל להיעזר ב-Event Viewer, כדי לצפות ביומני המעקב אשר נוצרים כתוצאה ממדיניות המעקב ומהאירועים המבוקרים. תוכל להשתמש ב-Event Viewer גם לשם צפייה בתוכן יומני אירועי האבטחה, ולאתר אירועים מסוימים בקבצי היומן.

שאלות סיכום

השאלות הבאות נועדו לחזק מידע מפתח שהוצג בפרק זה. אם אינך מסוגל לענות על שאלה, סקור את השיעור המתאים ונסה לענות על השאלה פעם נוספת. תשובות לשאלות תמצא בנספח A. לנוחיותך השאלות מופיעות באנגלית ואחר כך בעברית.

1. Which key is associated with the creation of digital signatures, the public key or the private key? Explain your answer.
2. What security credential(s) will be in use if you are supporting client computers running Windows 2000 and Windows NT that authenticate to servers running Windows 2000 Server, and Windows NT Server?
3. How can a security template be used to facilitate configuration and analysis of security settings?
4. Where is the Certificate Services Enrollment page and what is its purpose?
5. What steps must you follow to enable auditing of specific file objects on domain controllers in a domain where Group Policy is enabled?

1. איזה מפתח משויך ליצירת חתימות דיגיטליות, המפתח הציבורי או המפתח הפרטי? הסבר את תשובתך.
2. איזה נתוני אבטחה יהיו בשימוש, אם אתה תומך במחשבי לקוח הפועלים בסביבת Windows 2000 ו- Windows NT, המאמתים שרתים הפועלים בסביבת Windows 2000 Server ו- Windows NT Server?
3. כיצד יכולה תבנית אבטחה לסייע לקידום תצורה ולניתוח הגדרות אבטחה?
4. היכן נמצא הדף Certificate Services Enrollment ומה מטרתו?
5. איזה צעדים עליך לנקוט, כדי לאפשר ביצוע מעקב לאובייקט קובץ מסוים ב-DCs, ב-Domain בו מאופשרת מדיניות קבוצתית?

פרק 12

אמינות וזמינות

אודות פרק זה

שתיים מהדרישות החשובות ביותר עבור מערכת הפעלה עסקית הן אמינות וזמינות. בהקשר של מערכת הפעלה, **אמינות** (Reliability) מתייחסת למידת האחידות בה שרת מפעיל יישומים ושירותים, בעוד ש**זמינות** (Availability) מתייחסת לכמות הזמן בה ניתן להשתמש במערכת. אמינות מוגברת על ידי הפחתת הגורמים האפשריים לכשל המערכת. זמינות מוגברת על ידי התייחסות לגורמים לזמן ההשבתה. במילים אחרות, מערכות אמינות וזמינות עמידות בפני תקלות, וקל להפעילן מחדש לאחר השבתה. פרק זה מתמקד בתחזוקת התקני חומרה ומנהלי התקנים, גיבוי נתונים ויישום הגנה מפני אסון. בנוסף, מוצגת סקירה של מספר גישות להתאוששות מאסון, שיכולות לסייע במקרה של כשל במערכת.

לפני שתתחיל

לביצוע השיעורים בפרק זה, נדרש:

- Server01 המפעיל Microsoft Windows 2000 Server כ-DC.
- השלמת התרגילים בפרקים הקודמים.

שיעור 1: ניהול התקני חומרה ומנהלי התקנים

חומרה כוללת כל התקן פיסי, המחובר למחשב ומבוקר על ידי המיקרו-מעבד שלו. כדי שהתקן יפעל כראוי עם Windows 2000, יש לטעון למחשב מנהל התקן. **מנהל התקן** (Device Driver) הוא תוכנית המאפשרת להתקן מסוים לתקשר עם Windows 2000. למרות שהתקן כלשהו עשוי להיות מותקן במערכת, Windows 2000 לא תוכל להשתמש בהתקן עד להתקנה והגדרה של מנהל ההתקן (Driver) המתאים. שיעור זה מספק סקירה של חומרה, ומתאר כיצד לנהל התקנים ואת מנהלי ההתקנים שלהם. הפרק גם מתאר את הכלים הדרושים להוספה, הסרה והגדרה של התקנים ומנהלי התקנים אלה.

לאחר שיעור זה, תוכל

- **לנהל התקני חומרה ומנהלי התקנים על ידי שימוש באשף Add/Remove Hardware ובתוסף התוכנה Device Manager, על ידי הגדרת אפשרויות חתימת מנהל התקן ופרופילי חומרה, ועל ידי שימוש ביומני אירועים למעקב אמינות וזמינות.**
- להחיל עדכוני חבילת שירות (Service Pack).

זמן לימוד משוער: 40 דקות

סקירת חומרה

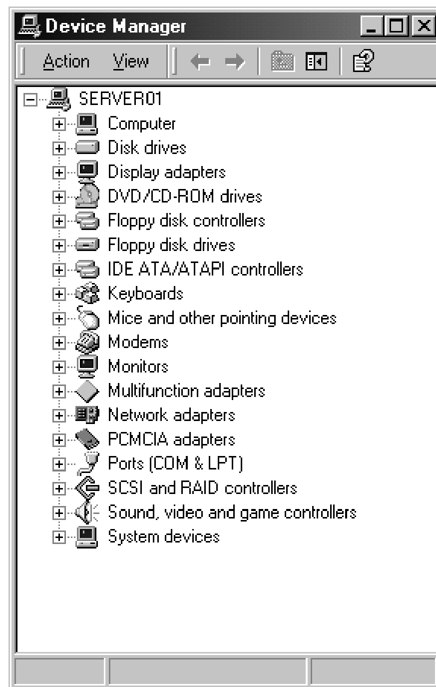
חומרה (Hardware) כוללת התקנים כלשהם שחוברו למחשב עם ייצורו, בנוסף לציוד היקפי אשר הוסף מאוחר יותר. לדוגמה, חומרת המערכת יכולה לכלול מודמים, כונני דיסק, בקרי דיסק, כונני תקליטורים, מדפסות, מתאמי רשת, מקלדות, צגים ומתאמי תצוגה (כרטיס מסך).

התקנים אלה, שיכולים להיות תואמים או לא תואמים לתקן Plug and Play (הכנס-הפעל), מחוברים למחשב במספר דרכים. חלק מההתקנים, כגון מתאמי רשת וכרטיסי קול, מחוברים לחריצי הרחבה בתוך המחשב. התקנים אחרים, כגון מדפסות וסורקים, מחוברים ליציאות בחלק החיצוני של המחשב, בעוד שהתקנים אחרים, המכונים PC Cards או PCMCIA, מתחברים רק לחריצי PC Card במחשב נייד.

לכל התקן יש מנהל התקן ייחודי לו, המסופק בדרך כלל על ידי יצרן ההתקן. רבים ממנהלי התקנים אלה נכללים בתקליטור ההתקנה של Windows 2000.

סוגי חומרה

Windows 2000 מסווגת התקנים על פי סוג חומרה. סוגי חומרה כוללים גורמים כגון מתאמי תצוגה, מקלדות, כונני תקליטורים, יציאות, ומדפסות. כאשר משתמשים בתוסף התוכנה Device Manager (תרשים 12.1) או באשף Add/Remove Hardware, מוצגת רשימת סוגי חומרה המותקנים במחשב.



תרשים 12.1 תוסף התוכנה Device Manager עבור המחשב המקומי.

סוגי חומרה מסווגים גם לפי התקנים שונים. לדוגמה, סוג החומרה מודם (Modem) כולל למעלה מ- 200 סוגי מודמים הניתנים להתקנה ושימוש עם Windows 2000.

התקנים ניתנים גם לסיווג לפי אופן חיבורם למחשב. מרבית ההתקנים מחוברים באופן קבוע למחשב, ומותקנים בדרך כלל רק פעם אחת. הם זמינים בכל פעם שמפעילים את המחשב, אלא אם מנתקים או מסירים אותם. התקנים המחוברים באופן קבוע כוללים:

- ❖ כרטיסי קול
- ❖ מתאמי תצוגה
- ❖ מודמים
- ❖ דיסקים קשיחים

התקנים אחרים מתוכננים להיות מחוברים ומנותקים מהמחשב לפי הצורך. ניתן לחבר או להכניס התקנים מסוג זה ליציאה או לחריץ ההרחבה המתאימים, ו-Windows 2000 תזהה את ההתקן ותגדיר אותו, ללא הפעלה מחדש של המחשב. באופן דומה, כאשר מנתקים התקנים מסוג זה, יש להודיע ל-Windows 2000 רק שמוציאים, מסירים או מנתקים את ההתקן. בדרך כלל אין צורך לכבות ולהפעיל מחדש את המחשב. התקנים המיועדים לחיבור וניתוק כוללים:

- PC Cards המתחברים למחשבים ניידים
- חומרה המתחברת ליציאת USB (Universal Serial Bus) או לאפיק IEEE 1394
- תחנות עגינה התומכות בעגינה ויציאה חמה של מחשבים ניידים
- חומרה המתחברת ליציאות טוריות (Serial) או מקביליות (Parallel)

לרשימה מקיפה של ההתקנים הנתמכים על ידי Windows 2000, ראה רשימת תאימות החומרה של HCL - Windows 2000 (**H**ardware **C**ompatibility **L**ist) על ידי ביצוע חיפוש לפי מילת המפתח HCL באתר האינטרנט של Microsoft (http://www.microsoft.com).

סקירה כללית של הכנס-הפעל

תקן **הכנס-הפעל** (**P**lug a**n**d **P**lay - PnP) עומד במערכת מפרטים שפותחה על ידי IEEE ויצרני מחשבים ותוכנה, כגון אינטל, קומפק, Microsoft, ו-Phoenix Technologies. מפרטים אלה מאפשרים למחשב לזהות ולהגדיר התקן אוטומטית, ולהתקין את מנהלי ההתקנים המתאימים. בעזרת Windows 2000, פשוט להתקין התקן PnP. נדרש רק לחבר את ההתקן למחשב, לספק מקור מתח חיצוני אם נדרש, ו-Windows 2000 עושה את כל השאר, על ידי התקנת מנהלי ההתקנים הדרושים, עדכון המערכת, והקצאת משאבי מערכת.

לדוגמה, ניתן לעגן מחשב נייד ולהתחבר לרשת מבלי לשנות את ההגדרות. מאוחר יותר, ניתן להוציא את אותו מחשב ולהשתמש במודם להתקשרות לרשת, שוב ללא ביצוע שינויים ידניים כלשהם להגדרות מערכת ההפעלה. Windows 2000 משנה אוטומטית את מצב מנהל ההתקן (device driver), כך שיתאים לתצורת החומרה החדשה (אם נעשה בה שינוי).

בעזרת הכנס-הפעל (Plug & Play), ניתן להיות בטוחים שהתקנים חדשים כלשהם יפעלו יחד כראוי, ושהמערכת תאתחל נכון לאחר התקנת חומרה או הסרתה. Windows 2000 גם מזהה חומרה חדשה כלשהי עם הפעלת המחשב, וטוענת את מנהלי ההתקנים הדרושים להתקן החומרה שאותר.

כאשר מתקינים או מסירים התקן חומרה, הכנס-הפעל עובד עם תוכנית השירות Windows 2000 Power Options, לניהול דרישות ההספק של החומרה וההתקנים ההיקפיים, על ידי כיבוי או חיסכון באנרגיה כאשר לא נעשה בהם שימוש. אם עובדים בתוכנית אחרת כאשר מתקינים או מסירים התקן, הכנס-הפעל מודיע שעומד להתבצע שינוי בהגדרות המחשב, ומזהיר שכדאי לשמור את השינויים.

אם משהו משתבש, רושם שירות יומן אירועים (Event Log) את המידע ביומן המערכת (System Log).

תמיכה במנהלי התקנים הכנס-הפעל

Windows 2000 מתקינה התקן הכנס-הפעל (Plug & Play device) ואת מנהל ההתקן (Device driver) שלו אוטומטית. אולם, אם תבחר להתקין Device driver ישן יותר או התקן חומרה מיושן, ייתכן שתקבל תמיכה מוגבלת בהכנס-הפעל, או שלא תקבל תמיכה כלל.

שימוש במנהל התקן הכנס-הפעל להתקנת התקן שאינו הכנס-הפעל עשוי לספק תמיכת הכנס-הפעל מסוימת. למרות שהמערכת אינה יכולה לזהות את החומרה ולטעון את מנהלי ההתקנים הדרושים לבדה, הכנס-הפעל יכול לפקח על ההתקנה על ידי הקצאת משאבים, אינטראקציה עם היישומון Power Options שבלוח הבקרה, ורישום נושאים כלשהם ביומן המערכת.

באופן כללי, לא ניתן להתקין חומרה שאינה הכנס-הפעל מבלי לבצע הגדרות ידניות כלשהן. השתמש באשף Add/Remove Hardware, או בתוסף התוכנה Device Manager לשינוי הגדרות התצורה עבור חומרה מיושנת.

התקנת התקנים

התקנת התקן חדש (Installing a new device) כוללת בדרך כלל שלושה שלבים:

1. חיבור ההתקן למערכת.
2. טעינת מנהלי ההתקנים הדרושים עבור ההתקן.
3. הגדרת המאפיינים וההגדרות של ההתקן.

כדי להבטיח פעולה נכונה של ההתקן, יש למלא אחר הוראות ההתקנה של יצרן ההתקן. הדבר עשוי לכלול כיבוי המחשב וניתוקו ממקור המתח, ואז חיבור ההתקן ליציאה המתאימה, או הכנסתו לחריץ המתאים.

אם ההתקן הוא הכנס-הפעל, או שהוא התקן חיוני להפעלה כגון כונן דיסק קשיח, הזיהוי מתבצע באופן אוטומטי. עם זאת, עבור התקנים מיושנים מסוימים, ייתכן שיהיה צורך להפעיל מחדש את המחשב, לאחר חיבור ההתקן למחשב. אז מנסה Windows 2000 לזהות את ההתקן החדש.

אם ההתקן אינו הכנס-הפעל, ייתכן שיהיה צורך להשתמש באשף Add/Remove Hardware בלוח הבקרה, כדי להורות ל-Windows 2000 מהו סוג ההתקן המותקן. לאחר זיהוי ההתקן על ידי Windows 2000 או באמצעות האשף Add/Remove Hardware, ייתכן שתתבקש להכניס את תקליטור ההתקנה של Windows 2000, או דיסקט, או את התקליטור של היצרן, לצורך טעינת מנהלי ההתקנים הדרושים.

לאחר טעינת מנהלי ההתקנים למערכת, Windows 2000 מגדירה את המאפיינים וההגדרות עבור ההתקן. למרות שניתן להגדיר ידנית את המאפיינים וההגדרות של התקנים, מומלץ לאפשר ל-Windows 2000 לעשות זאת. כאשר ההגדרה מתבצעת ידנית, ההגדרות יהיו קבועות, ופירוש הדבר ש-Windows 2000 לא תוכל לשנות אותן בעתיד, אם תתעורר בעיה כלשהי או סתירה מול הגדרות של התקן אחר.

להתקנת ההתקן, חבר אותו ליציאה או לחריץ המתאימים במחשב בהתאם להוראות יצרן ההתקן. ייתכן שיהיה צורך להפעיל מחדש את המחשב. עליך להיכנס למערכת כמנהל, או כחבר בקבוצה Administrators, להשלמת הליך זה. אולם, אם משתמש בעל הרשאות מנהל כבר טען את מנהלי ההתקנים עבור התקן מסוים, תוכל להתקין את ההתקן ללא הרשאות מנהל. שים לב גם שהגדרות מדיניות רשת עלולות למנוע ממך להשלים הליך זה אם המחשב מחובר לרשת.

במצב בו יש להפעיל מחדש את המחשב, Windows 2000 צריכה לזהות את ההתקן ולהפעיל את האשף Found New Hardware. בעת התקנת התקן, כמו למשל התקנת כרטיס קול לתוך חריץ הרחבה בלוח האם, סגור את Windows, כבה את המחשב ונתק אותו ממקור המתח (הדבר חשוב בעיקר בעת העבודה עם מחשבים מבוססי לוח אם ATX). הסר את כיסוי המחשב והתקן את ההתקן בחריץ ההרחבה המתאים. החזר את כיסוי המחשב, חבר אותו למתח והפעל את המחשב.

אם ההתקן אינו מותקן כהלכה, ייתכן שזהו התקן מיושן יותר, שאינו הכנס-הפעל. מלא אחר ההוראות על המסך (אם יש) לבחירת נתיב יעד להתקנת מנהלי ההתקנים עבור ההתקן.

אם ההתקן הוא מסוג SCSI (**S**mall **C**omputer **S**ystem **I**nterface), חבר אותו ליציאת בקר SCSI במחשב, בהתאם להוראות יצרן ההתקן. הפעל מחדש את המחשב. יש לוודא שמספר ההתקן עבור התקן SCSI זה, אינו בשימוש על ידי התקן SCSI אחר, ושלהתקן יש נגד-סיום (Termination) מתאים. לשינוי מספר ההתקן, ראה הוראות של יצרן ההתקן.

הערה ייתכן שכרטיסי בקר SCSI בתקן PCMCIA (**P**ersonal **C**omputer **M**emory **C**ard **I**nternational **A**ssociation) והתקנים אחרים אינם דורשים הפעלה מחדש של המחשב לאחר התקנתם. כמו תמיד, יש להתייחס להוראות היצרן בעת התקנת חומרה. יש להתייחס למידע המסופק בפרק זה כהנחיות כלליות להתקנת חומרה.

אם ההתקן הוא התקן USB או IEEE 1394, הכנס אותו ליציאת USB או IEEE כלשהי במחשב. מלא אחר ההוראות על המסך. אין צורך לכבות או לנתק את המחשב בעת התקנה או חיבור התקן USB או IEEE 1394. למרות ש-USB ו-IEEE 1394 הן טכנולוגיות דומות, לא ניתן להחליף בין חיבורי USB לחיבורי IEEE 1394.

הסרת התקנים

בדרך כלל ניתן לבטל התקנת התקן הכנס-הפעל על ידי ניתוקו או הסרתו. עבור התקנים אחדים, ייתכן צורך לכבות תחילה את המחשב. כדי להבטיח ביצוע נכון, יש לפעול לפי הוראות ההתקנה וההסרה של היצרן.

ניתן להשתמש באשף Add/Remove Hardware או בתוסף התוכנה Device Manager, כדי ליידע את Windows 2000 שרוצים להסיר התקנה של התקן שאינו הכנס-הפעל. לאחר הודעה ל-Windows 2000 על הסרת התקן, יש לנתק או להסיר פיסית את ההתקן מהמחשב. לדוגמה, אם ההתקן מחובר ליציאה חיצונית למחשב, יש לכבות את המחשב, לנתק את ההתקן מהיציאה, ואז לנתק את כבל המתח שלו, אם קיים.

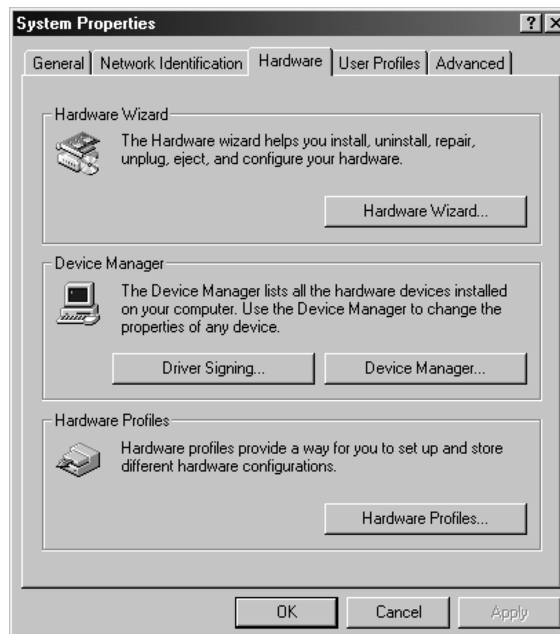
במקום להסיר התקנה של התקן הכנס-הפעל שעשוי להיות מחובר שוב בעתיד, כגון מודם, ניתן לנטרל התקן. כאשר מנטרלים התקן, ההתקן הפיסי נשאר מחובר למחשב, אולם Windows 2000 מעדכנת את רישום המערכת (System Registry) כך שמנהלי ההתקנים אינם נטענים עוד כאשר מאתחלים את המחשב. כאשר מפעילים את ההתקן, מנהלי ההתקן זמינים שוב. נטרול התקנים הוא צעד מועיל אם רוצים יותר מאשר תצורת חומרה יחידה (פרופיל חומרה) עבור המחשב. שימוש במספר פרופילי חומרה נפוץ עבור מחשבים ניידים הפועלים הן עם תחנת עגינה והן בלעדיה.

הערה תוסף התוכנה Device Manager **אינו** מסיר מנהלי התקנים מהדיסק הקשיח. אם רוצים לעשות זאת, **יש** להשתמש באשף Add/Remove Hardware, **ולבחור** את האפשרות Uninstall A Device Removal Task. בנוסף, **יש** לבדוק בתיעוד היצרן של ההתקן מה הדרך הנכונה ביותר להסרת מנהלי התקנים.

כלים לניהול התקנים ומנהלי התקנים

קיימים מספר כלים לניהול התקני חומרה (Hardware devices) ומנהלי ההתקנים (Drivers) שלהם. למרבית כלים אלה ניתן לגשת באמצעות הכרטיסיה Hardware שבתיבת הדו-שיח System Properties. לפתיחת תיבת הדו-שיח System Properties, פתח את לוח הבקרה (Control Panel), ואז פתח את היישום System, או החזק לחוץ את מקש Windows והקש על המקש Break. עם הצגת תיבת הדו-שיח System Properties, בחר את הכרטיסיה Hardware (תרשים 12.2).

מכאן, ניתן לפתוח את אשף Add/Remove Hardware, את תוסף התוכנה Device Manager, את תיבת הדו-שיח Driver Signing Options, ואת תיבת הדו-שיח Hardware Profiles. בנוסף לכלים אלה, שאליהם ניתן לגשת דרך תיבת הדו-שיח System Properties, ניתן להשתמש ביומני מציג האירועים (Event Viewer) לאיתור תקלות בתצורות חומרה.



תרשים 12.2 תיבת הדו-שיח System Properties והכרטיסיה Hardware.

אשף Add/Remove Hardware

אשף Add/Remove Hardware מאפשר הוספת חומרה חדשה, ניתוק או הסרת חומרה מהמחשב, או איתור תקלות הקשורות לחומרה (תרשים 12.3).



תרשים 12.3 מסך הפתיחה של אשף Add/Remove Hardware.

בנוסף לאפשרות לפתוח את האשף מהכרטיסיה Hardware של תיבת הדו-שיח System Properties, ניתן לפתוח אותו מלוח הבקרה על ידי בחירה ב- Add/Remove Hardware. לאחר פתיחת האשף, מלא אחר ההוראות באשף להוספה, הסרה, ניתוק, או איתור תקלות בחומרה.

הערה לשימוש באשף Add/Remove Hardware, עליך להיות מחובר אל, או לפעול בהקשר של חשבון בעל הרשאות אדמיניסטרטיביות. השתמש בתוכנית השירות Runas משורת הפקודה לפעולה בהקשר האבטחה של חשבון משתמש אחר. אם המחשב מחובר לרשת, הגדרות מדיניות רשת עלולות למנוע אפשרות שימוש באשף Add/Remove Hardware.

תוסף התוכנה Device Manager

Device Manager הוא תוסף תוכנה של MMC Console, המספק תצוגה גרפית של החומרה המותקנת על המחשב (תרשים 12.1).

בנוסף לאפשרות לפתוח את תוסף התוכנה Device Manager מהכרטיסיה Hardware שבתיבת הדו-שיח System Properties, ניתן לפתוח את הכלי מה- Computer Management console או ליצור MMC Console מותאם אישית, המכיל את תוסף התוכנה Device Manager. לאחר פתיחת Device Manager, ניתן להשתמש בו לשינוי אופן הגדרת החומרה בנוסף לאופן האינטראקציה של החומרה עם מעבד המחשב.

תוסף התוכנה Device Manager מאפשר לבצע את הפעולות הבאות:

- ❖ לקבוע האם החומרה במחשב פועלת כראוי.
- ❖ לשנות הגדרות תצורת חומרה.
- ❖ לזהות את מנהלי ההתקנים הטעונים עבור כל התקן, ולקבל מידע אודות כל מנהל התקן.
- ❖ לשנות הגדרות מתקדמות ומאפיינים עבור התקנים.
- ❖ להתקין מנהלי התקנים מעודכנים.
- ❖ לנטרל, להפעיל ולהסיר התקנה של התקנים.
- ❖ לזהות סתירות Device, ולהגדיר ידנית הגדרות משאבים.
- ❖ להדפיס דוח משאבי מערכת של ההתקנים המותקנים במחשב.

בדרך כלל, Device Manager משמש לבדיקת מצב חומרה ולעדכון מנהלי התקנים. משתמשים מתקדמים, בעלי הבנה יסודית של חומרת מחשב, גם משתמשים בתכונות האבחון של Device Manager לפתרון סתירות בין התקנים ולשינוי הגדרות משאבים.

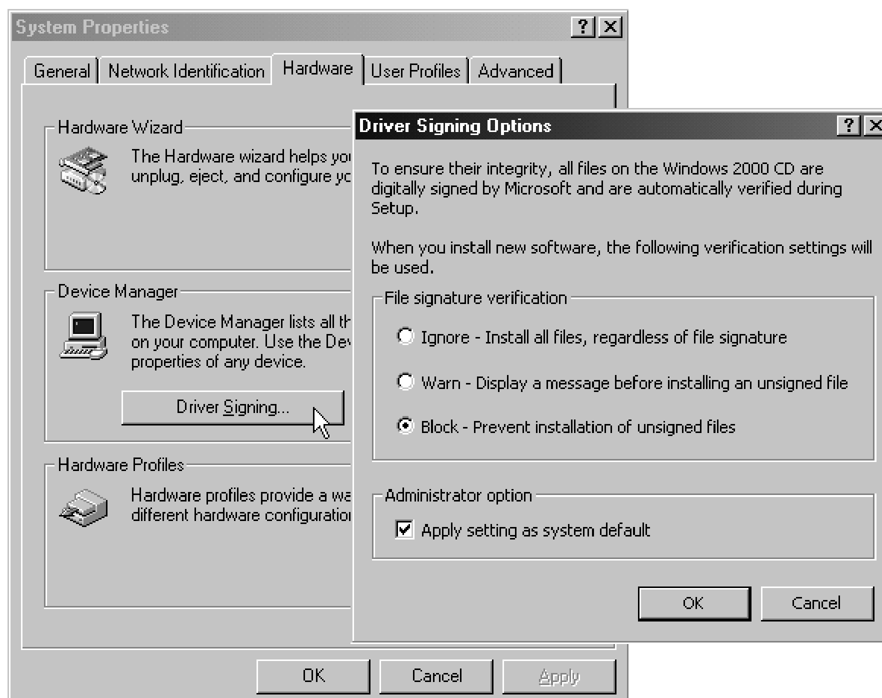
חשוב שינוי הגדרות משאבים באופן לא נכון, עלול לנטרל את החומרה, ולגרום לתקלות בפעולת המחשב, או אף למנוע את יכולת המחשב לפעול. רצוי שרק משתמשים שיש להם מומחיות בחומרת מחשבים ובהגדרות חומרה ישנו הגדרות משאבים.

בדרך כלל, לא יהיה צורך להשתמש בתוסף התוכנה Device Manager לשינוי הגדרות משאבים, מכיון שמשאבים מוקצים באופן אוטומטי על ידי Windows 2000 במהלך הגדרות החומרה. בנוסף, Device Manager יכול לשמש לניהול התקנים במחשב מקומי בלבד. על מחשב מרוחק, Device Manager פועל במצב קריאה בלבד.

הערה לשימוש בתוסף התוכנה Device Manager, עליך להיות מחובר אל או לפעול בהקשר של חשבון בעל הרשאות אדמיניסטרטיביות. אם המחשב מחובר לרשת, הגדרות מדיניות רשת עלולות למנוע אפשרות שימוש באשף Add/Remove Hardware.

חתימת מנהלי התקנים

תכונת Driver Signing מאפשרת ל-Windows 2000 להודיע למשתמשים האם מנהל התקן שהם מתקינים עבר את הליך האישור של Microsoft (תרשים 12.4). Driver Signing מצמיד חתימה דיגיטלית מוצפנת לקובץ קוד אשר עבר את בדיקות מעבדות איכות חומרת Windows - WHQL (**W**indows **H**ardware **Q**uality **L**abs).



תרשים 12.4 תיבת הדו-שיח Driver Signing Options.

Microsoft חותמת דיגיטלית על מנהלי התקנים, כחלק מבדיקות WHQL, אם ה-Device driver פועל על מערכות הפעלה Windows 2000. החתימה הדיגיטלית משוייכת ל-Individual driver packages ומוכרת על ידי Windows 2000. הליך אישור זה מוכיח למשתמשים, שמנהלי ההתקנים (Drivers) שהם מפעילים זהים לאלה ש-Microsoft בדקה, ומודיע להם אם קובץ מנהל ההתקן (Device driver) שונה לאחר שמנהל ההתקן הוצב ברשימת HCL.

אפשרות Driver Signing מאפשרת שלוש תגובות:

- **Ignore** – מאפשר התקנת כל הקבצים, בין אם הם חתומים ובין אם לא.
- **Warn** – מודיע למשתמש אם מנהל התקן המותקן כעת לא נחתם, ומאפשר למשתמש הזדמנות לומר "לא" להתקנה. מצב זה גם מספק למשתמש אפשרות להתקין גרסאות לא חתומות של קובץ מנהל התקן מוגן.
- **Block** – מונע התקנה של כל מנהלי ההתקנים שאינם חתומים.

Windows 2000 משווקת, כאשר מצב Warn מוגדר כברירת מחדל .

Driver Signing אינו משפיע על הקוד עצמו. אלא, Microsoft חותמת על הקוד הבינרי של מנהל ההתקן אשר עובר את בדיקות WHQL. אז Microsoft מייצרת קובץ קטלוג המכיל את הקוד וחתימה דיגיטלית מוצפנת. הקובץ הבינרי הנוצר בנוי באופן שאינו מאפשר לשנות את הקוד, מבלי שחתימת קובץ הקטלוג תהפוך לבלתי תקפה.

הערה למידע נוסף אודות חתימות דיגיטליות והצפנה, ראה פרק 11.

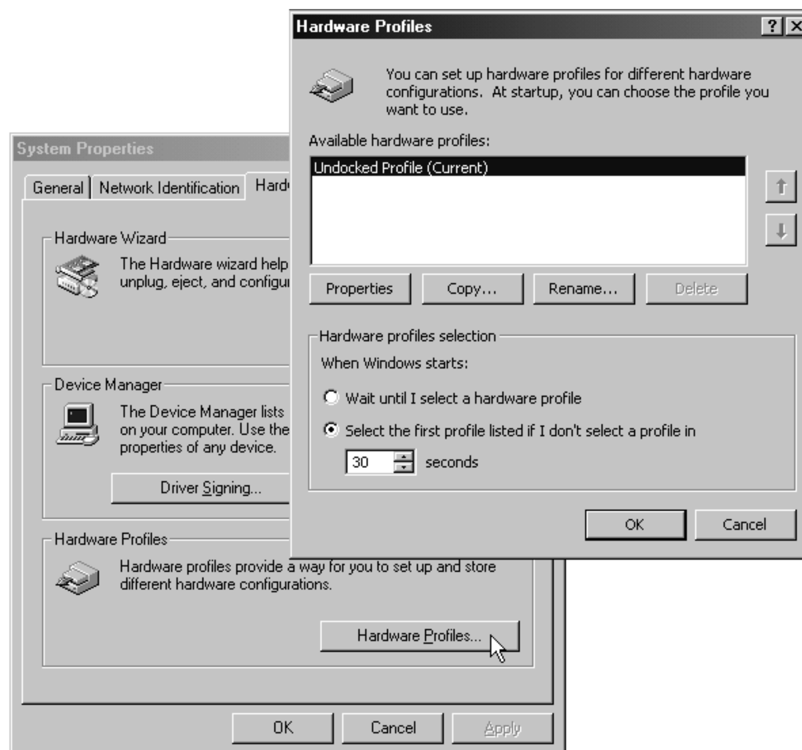
למעשה, הצפנה (Hash) של מנהל ההתקן הבינרי והמידע הרלוונטי מאוחסנים בקובץ קטלוג (cat), וקובץ cat זה נחתם בחתימה הדיגיטלית של Microsoft. הקוד הבינרי עצמו אינו עובר שינוי; רק קובץ cat מיוצר עבור כל חבילת מנהל התקן. הקשר בין חבילת מנהל ההתקן לבין קובץ cat שלו מוזכר בקובץ inf. של מנהל ההתקן, ונשמר על ידי המערכת לאחר התקנת מנהל ההתקן.

ספקים הרוצים שמנהלי ההתקנים שלהם ייבדקו וייחתמו, יכולים למצוא מידע אודות חתימת מנהלי התקנים בכתובת /http://www.microsoft.com/hwdev. רק מנהלי התקנים חתומים מפורסמים באתר Windows Update בכתובת http://windowsupdate.microsoft.com/default.htm.

הערה אם אתה מחובר אל או פועל בהקשר של חשבון בעל הרשאות אדמיניסטרטיביות, סמן את תיבת הסימון Apply Setting As System Default (תרשים 12.4), להחלת ההגדרה שנבחרה כברירת המחדל עבור כל המשתמשים הנכנסים למחשב. אפשרויות Driver Signing ניתן להגדיר גם ב-Group Policy, על ידי בחירת הגדרת האבטחה Unsigned Driver Installation Behavior.

פרופילי חומרה

פרופיל חומרה הוא מערכת הוראות המורה ל-Windows 2000 איזה התקנים להפעיל עם הפעלת המחשב, או באילו הגדרות להשתמש עבור כל התקן. עם ההתקנה הראשונה של Windows 2000, נוצר פרופיל חומרה בשם Profile 1 (Current). שם פרופיל ברירת המחדל שונה במחשבים ניידים. שם נפוץ הניתן למחשבים ניידים, כברירת מחדל, הוא Undocked Profile (Current) (פרופיל ללא עגינה), כמתואר בתרשים 12.5.



תרשים 12.5 תיבת הדו-שיח Hardware Profiles.

כברירת מחדל, כל התקן המותקן במחשב בעת התקנת Windows 2000 מופעל בפרופיל חומרה ברירת המחדל.

פרופילי חומרה שימושיים במיוחד, אם משתמשים במחשב נייד. מרבית המחשבים הניידים משמשים במיגוון מיקומים, ופרופילי חומרה מאפשרים לשנות את ההתקנים המשמשים את המחשב כאשר הוא מועבר ממקום למקום. לדוגמה, ניתן להגדיר פרופיל אחד בשם Docking Station Configuration לשימוש במחשב הנייד בתחנת עגינה עם רכיבי חומרה, כגון כונן תקליטורים ומתאם רשת. ניתן להגדיר גם פרופיל נוסף בשם Undocked Configuration לשימוש במחשב הנייד בבית מלון או במטוס, כאשר לא משתמשים במתאם רשת או כונן תקליטורים, אך משתמשים במודם ובמדפסת ניידת.

ניתן לנהל פרופילי חומרה על ידי פתיחת System ב-Control Panel, בחירה בכרטיסיה Hardware, ולחיצה על Hardware Profiles. אם יש יותר מפרופיל חומרה יחיד, ניתן לציין פרופיל ברירת מחדל שישמש עם כל הפעלה של המחשב. ניתן גם לגרום ל- Windows 2000 לשאול באיזה פרופיל להשתמש בכל פעם שמפעילים את המחשב. לאחר יצירת פרופיל חומרה, ניתן להשתמש ב- Device Manager לנטרול והפעלת התקנים בפרופיל. כאשר מנטרלים התקן בפרופיל חומרה, מנהלי ההתקנים עבור התקן זה אינם נטענים עם הפעלת המחשב.

הערה עליך להיות מחובר אל או לפעול בהקשר של חשבון בעל הרשאות אדמיניסטרטיביות במחשב המקומי ליצירה, העתקה, שינוי שם, או מחיקת פרופילי חומרה.

הפרופיל הנוצר עם התקנת Windows 2000 (פרופיל התקנה) מהווה דגם שעל פיו ניתן ליצור פרופילי חומרה חדשים. כדי לגרום לפרופיל חומרה להופיע לאחר יצירתו, יש לגשת למאפייני הפרופיל ולסמן את תיבת הסימון Always Include This Profile As An Option When Windows Starts.

יומני אירועים

מעקב זהיר אחר יומן המערכת (System Log), הנוצר על ידי השירות Event Log, יכול לסייע לחזות ולזהות את המקורות של בעיות מערכת. לדוגמה, אם אזהרות היומן מורות שמנהל התקן דיסק יכול לכתוב למקטע רק לאחר מספר ניסיונות, סביר שלאורך זמן מקטע זה לא יהיה תקין.

יומני יישום (Application Log) ומערכת (System Log) יכולים לאשר בעיות תוכנה. אם תוכנית כושלת, יומן יישום יכול לספק רישום של הפעילות שהובילה לאירוע.

ההצעות הבאות עשויות לסייע בשימוש ביומני אירועים לאבחון תקלות:

- **אחסון יומנים בתבנית יומן** – הנתונים הבינריים הקשורים לאירוע נשמרים, אם מאחסנים את היומן בתבנית יומן (.evt), אולם מושלכים אם מאחסנים נתונים בתבנית טקסט (.txt) או בפורמט ערכים מופרדים בפסיקים (.csv). הנתונים הבינריים עשויים לסייע לאיש פיתוח, או למומחה תמיכה טכנית, לזהות את מקור הבעיה.
- **שים לב לקודים של זיהוי אירועים** – מספרים אלה תואמים לתיאור טקסט בקובץ הודעה. המספרים יכולים לשמש לנציגי תמיכה במוצר, להבנה מה אירע במערכת.
- **התייחס לבעיות חומרה** – אם יש חשד שרכיב חומרה הוא המקור לבעיות מערכת, סנן את יומן המערכת, להצגת האירועים שנוצרו על ידי רכיב זה בלבד.
- **התייחס לבעיות מערכת** – אם אירוע מסוים נראה קשור לבעיות מערכת, נסה לחפש ביומן האירועים לאיתור מקרים נוספים של אותו אירוע, או למציאת תדירות השגיאה.

הערה למידע נוסף אודות השימוש ביומני אירועים, ראה בתקליטור המצורף לספר זה (\chapt12\articles\Monitoring Reliability.doc).

התקנת חבילות שירות

Windows 2000 מקלה על מנהלים בהוספת חבילות שירות (Service Pack). ב- Windows NT, Windows 95 ו- Windows 98, חבילות שירות מותקנות בנפרד, לאחר התקנת מערכת ההפעלה. Windows 2000 תומכת ב-slipstreaming (זרימה חלקה של הטמעה) של חבילות שירות, ופירוש הדבר שחבילת השירות מוחלת ישירות בעת הפצת השיתוף של מערכת ההפעלה במהלך ההתקנה.

Windows 2000 גם מונעת את הצורך להתקין מחדש רכיבים שהוחלו לפני התקנת חבילת שירות. כך קל הרבה יותר להתקין חבילות שירות על מערכות קיימות. בעבר, עם התקנת חבילות שירות, היה צורך להתקין מחדש רכיבים רבים שהותקנו קודם לכן. לדוגמה, כאשר מוחלת חבילת שירות על Windows NT 4.0, שירותים שהותקנו קודם לכן, כגון IPX או RAS, חייבים להיות מותקנים מחדש. כדי להתייחס לבעיות שהיו קיימות עם חבילות שירות של Windows NT 4.0, Windows 2000 מספקת הטמעה חלקה של חבילות שירות והתקנת חבילות שירות לאחר הליך ההתקנה.

Slipstreaming של חבילות שירות

slipstreaming של חבילות שירות מתייחס לחבילת שירות, המוחלת על קבצי הפצה של Windows 2000 על תקליטור, או על שיתוף של רשת. כאשר Windows 2000 מותקנת מאחד ממקורות אלה, הקבצים המתאימים מחבילת השירות מותקנים, ללא צורך בהחלה ידנית של חבילת השירות לאחר ההתקנה.

כדי להחיל חבילת שירות חדשה, השתמש ב- update.exe עם מתג s:distribution_Folder -. כאשר distribution_Folder מייצג את שם התיקיה שתכיל את קבצי ההתקנה של Windows 2000. פעולה זו מעתיקה את קבצי חבילת השירות המעודכנת על פני קבצי Windows 2000 הקיימים. בין קבצי המפתח המוחלפים נכללים:

- קבצי layout.inf, dosnet.inf ו-txtsetup.sif חדשים הכוללים סכומי ביקורת (Checksums) עבור כל קבצי חבילת השירות. קבצים אלה זקוקים לערכים נוספים אם מוסיפים קבצים נוספים.
- קובץ driver.cab חדש, אם מנהלי ההתקנים בקובץ הארכיון (cabinet) משתנים.

התקנה של חבילת שירות לאחר הליך ההתקנה

חבילת שירות מוחלת על מערכת Windows 2000 קיימת על ידי הפעלת update.exe ועדכון המערכת ל-Windows 2000 בתוספת חבילת השירות. כאשר משתנה מצב המערכת (לדוגמה, על ידי הוספה או הסרה של שירותים), מערכת הבסיס מקבלת הודעה שהותקנה חבילת שירות, שקבצים הוחלפו או עודכנו על ידי חבילת השירות, ומהיכן הותקנה חבילת השירות. פירוש הדבר שהקבצים הנכונים מועתקים ממיקום ההפצה של חבילת השירות (שיתוף הרשת, התקליטור, או אתר האינטרנט) וממקור

ההתקנה של Windows 2000 (שיתוף הרשת או תקליטור). הדבר מונע את הצורך להחיל מחדש חבילת שירות כאשר משתנה מצב המערכת.

לאחר החלת חבילת שירות, אם משתנה מצב המערכת (לדוגמה, מוסיפים RAS לאחר החלת חבילת השירות), Windows 2000 מתקינה את הקבצים הנכונים, בין אם מקור קבצים אלה הוא בתקליטור Windows 2000, או בחבילת השירות. שוב, הדבר מונע את הצורך להחיל מחדש את חבילת השירות, עם כל שינוי של מצב המערכת.

סיכום שיעור

חומרה כוללת כל התקן פיסי המחובר למחשב והנשלט על ידי מעבד המחשב. מנהל התקן מאפשר להתקן מסוים לתקשר עם Windows 2000. Windows 2000 מסווגת התקנים לפי סוג חומרה. התקן הכנס-הפעל (Plug and Play) תואם למערכת מפרטים, המאפשרים למחשב לזהות ולהגדיר אוטומטית את ההתקן ולהתקין את מנהלי ההתקנים הדרושים. התקנת התקן חדש כרוכה בדרך כלל בשלושה שלבים: חיבור ההתקן למחשב, טעינת מנהלי ההתקן המתאימים עבור התקן זה, והגדרת מאפיינים והגדרות של ההתקן. בדרך כלל ניתן להסיר התקן הכנס-הפעל על ידי ניתוק או הרחקת ההתקן. ניתן להשתמש באשף Add/Remove Hardware או בתוסף התוכנה Device Manager כדי להודיע ל-Windows 2000 שרוצים להסיר התקנה של התקן שאינו הכנס-הפעל. קיימים מספר כלים לניהול התקני חומרה ומנהלי ההתקנים שלהם. מהכרטיסיה Hardware של תיבת הדו-שיח System Properties, ניתן לפתוח את אשף Add/Remove Hardware, את תוסף התוכנה Device Manager, את תיבת הדו-שיח Driver Signing Options, ואת תיבת הדו-שיח Hardware Profiles. בנוסף לכלים שאליהם ניתן לגשת דרך תיבת הדו-שיח System Properties, ניתן להשתמש ביומן אירועים (Event Log) לאיתור תקלות בהגדרות תצורת חומרה. ניתן לשלב עדכוני חבילות שירות ברשת, כך שהתקנות חדשות של Windows 2000 מחילות את עדכוני חבילות השירות, כחלק מהליך ההגדרה. שינויים בהגדרות של מערכות Windows 2000 קיימות, מחילים אוטומטית את עדכוני חבילות השירות.

שיעור 2: גיבוי נתונים

המטרה של כל פעולות הגיבוי היא להבטיח שניתן יהיה לשחזר נתונים אבודים ביעילות ובמהירות. פעולת גיבוי היא הליך יחיד של גיבוי נתונים. גיבוי סדיר של נתונים על דיסקים קשיחים של השרת ועל דיסקים קשיחים של המחשב, מונע אובדן נתונים, כתוצאה מכשל בכונני דיסקים, הפסקות חשמל, הידבקות בווירוסים ואירועים דומים. במקרה של אובדן נתונים, אם בוצעו פעולות גיבוי סדירות שתוכננו היטב, ניתן לשחזר את הנתונים האבודים, בין אם הם קובץ יחיד או דיסק קשיח שלם.

לאחר שיעור זה, תוכל

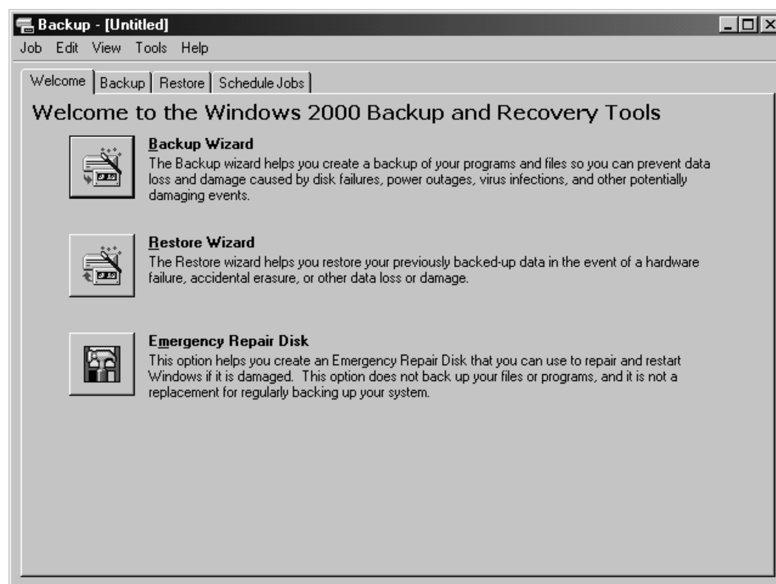
- לגבות נתונים במחשב ועל פני הרשת.
- לתזמן פעולת גיבוי.
- להגדיר אפשרויות גיבוי עבור Windows Backup.

זמן לימוד משוער: 60 דקות

מבוא ל- Windows Backup

Windows 2000 מספקת את Windows Backup (תרשים 12.6), שהוא כלי המאפשר גיבוי ושחזור נתונים בקלות. להפעלת Windows Backup, בתפריט Start, הצבע על Programs, הצבע על Accessories, הצבע על System Tools, ולחץ על Backup; או, בתפריט Start, לחץ על Run, הקלד **ntbackup**, ולחץ OK.

ניתן להשתמש ב-Backup לגיבוי ידני של נתונים, או לתזמון פעולות גיבוי סדירות ללא השגחה. ניתן לגבות נתונים בדיסק קשיח, בדיסקים ניתנים להסרה (כגון כונני Iomega Zip וכונני Jaz), בתקליטורים המאפשרים הקלטה, בכוננים אופטיים ובטייפים.



תרשים 12.6 הכרטיסיה Welcome של תיבת הדו-שיח Backup.

לגיבוי ושחזור מוצלחים של נתונים על מחשב המפעיל Windows 2000, עליך להיות בעל הרשאות וזכויות משתמש מתאימות, כמוסבר להלן:

- כל משתמש יכול לגבות את הקבצים והתיקיות שבבעלותו. משתמשים יכולים גם לגבות קבצים שעבורם יש להם הרשאות הכוללות את Read כגון Read, Read & Execute, Modify או Full Control (קריאה, קריאה וביצוע, שינוי, או שליטה מלאה).
- כל משתמש יכול לשחזר קבצים ותיקיות שעבורם יש לו הרשאות הכוללות את Write כגון Write, Modify או Full Control (כתיבה, שינוי, או שליטה מלאה).
- חברים בקבוצות Administrators, Backup Operators, ו- Server Operators יכולים לגבות ולשחזר את כל הקבצים (ללא תלות בהרשאות המוקצות). כברירת מחדל, חברים בקבוצות אלה מקבלים את הרשאות המשתמש Backup Files And Directories ו- Restore Files And Directories (גבה קבצים וספריות, ושחזר קבצים וספריות).

תכנון נושאים עבור Windows Backup

יש לתכנן את פעולות הגיבוי, כך שיתאימו לצרכי החברה. המטרה העיקרית בגיבוי נתונים היא יכולת לשחזר אותם במקרה הצורך, כך שכל תוכנית גיבוי שתפתח צריכה לכלול גם את אופן שחזור הנתונים. יש לדאוג ליכולת לשחזר במהירות ובהצלחה נתונים קריטיים אבודים. אין תוכנית גיבוי יחידה נכונה עבור כל הרשתות. הסעיפים הבאים עוסקים בנושאים שיש לשקול בעת גיבוש תוכנית הגיבוי.

קבע איזה קבצים ותיקיות יש לגבות

יש לגבות תמיד קבצים ותיקיות קריטיים הדרושים לחברה לצורך פעולתה, כגון רשומות מכירות וכספים, את רישום המערכת (System Registry) של כל שרת, ואת Active Directory store (מחסן Active Directory).

קבע את תדירות הגיבוי

אם הנתונים קריטיים לפעולת החברה, גבה אותם על בסיס יומי. אם משתמשים יוצרים או משנים דוחות פעם בשבוע, מספיק לגבות את הדוחות מדי שבוע. יש צורך לגבות נתונים לפי התדירות בה הם משתנים. לדוגמה, אין צורך לבצע גיבוי יומי לקבצים שמשתנים לעיתים רחוקות, כגון דוחות חודשיים.

קבע באיזה אמצעי להשתמש לאחסון נתוני הגיבוי

בעזרת Windows Backup, ניתן לגבות לאמצעים הבאים, הניתנים להסרה:

- **קבצים** – ניתן לאחסן את הקבצים על דיסק מקומי אך מומלץ לגבות אותם על אמצעי ניתן להסרה, כגון כונן Iomega Zip, או שיתוף ברשת, כגון שרת קבצים. הקובץ הנוצר מכיל את הקבצים והתיקיות שבחרת לגבות. לקובץ יש סיומת bkf. משתמשים יכולים לגבות את הנתונים האישיים שלהם לשרת רשת.
- **טייפ** – אמצעי פחות יקר מאמצעים אחרים הניתנים להסרה, טייפ נוח יותר עבור עבודות גיבוי גדולות הודות לקיבולת האחסון הגדולה שלו. אולם, לטייפ יש אורך חיים מוגבל ואיכותו עלולה להידרדר. הקפד לבדוק את המלצות היצרן לשימוש בטייפ.

הערה אם משתמשים בהתקן אחסון הניתן להסרה לצורך גיבוי ושחזור נתונים, יש להקפיד ולבדוק שההתקן נתמך ברשימת Windows 2000 HCL.

קבע האם לבצע גיבוי רשת או גיבוי מקומי

משמעות גיבוי רשת היא חיבור אמצעי האחסון אל השרת וגיבוי הנתונים ממחשבים מרוחקים, דרך הרשת. במצב זה שומרים המשתמשים את הנתונים שלהם במחשב המקומי ממנו הם פועלים. גיבוי רשת מאפשר איחוד נתוני גיבוי ממספר מחשבים לאמצעי גיבוי יחיד הניתן להסרה. גיבוי רשת גם מאפשר למנהל אחד לגבות את הרשת כולה. ההחלטה אם לבצע גיבוי רשת או גיבוי מקומי, תלויה בנתונים אותם יש לגבות. לדוגמה, עבור רישום המערכת (Registry) ו- Active Directory store, ניתן לבצע רק גיבוי מקומי במחשב אליו מחובר התקן הגיבוי וממנו מבצעים את הגיבוי.

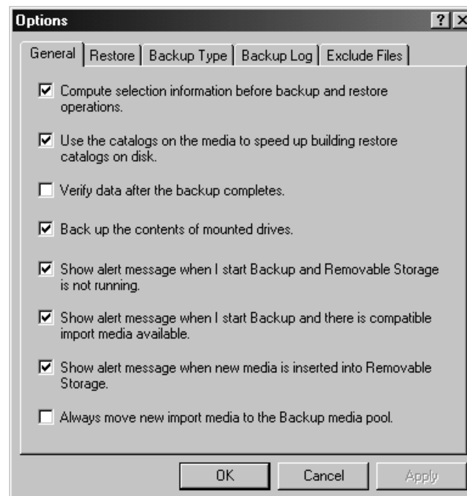
אם מחליטים לבצע גיבויים מקומיים, יש לבצע אותם בכל אחד מהמחשבים, כולל שרתים ומחשבי לקוח. יש להתייחס למספר נושאים בעת ביצוע גיבויים מקומיים. ראשית, יש לעבור ממחשב למחשב, כדי שניתן יהיה לבצע גיבוי בכל מחשב, או שיש לסמוך על המשתמשים שיגבו את המחשבים שלהם. בדרך כלל, מרבית המשתמשים אינם מגבים את הנתונים שלהם באופן סדיר. שיקול נוסף בגיבויים מקומיים הוא מספר התקני האחסון הניתנים להסרה הזמינים. אם משתמשים בהתקני אחסון ניתנים להסרה, כגון כונני טייפ, חייב להיות טייפ אחד עבור כל מחשב, או שיש להעביר את כונן הטייפ ממחשב למחשב, כדי לבצע גיבוי מקומי בכל מחשב.

אם מחליטים לבצע גיבוי מקומי על השרת בלבד, יש לדאוג לכך שהמשתמשים ישמרו את הנתונים שלהם על שיתוף בשרת (כגון Home Folder). שמירת נתוני המשתמשים על שרת קבצים יעילה עבור ניהול וגיבוי מרוכזים, אך יש להתייחס למספר נושאים בשיטה זו הנוגעים לתעבורת הרשת במשך שעות העבודה וכן לדאוג לנפח דיסק גדול מספיק של השרת.

ניתן גם לבחור להשתמש בשילוב של פעולות גיבוי רשת וגיבוי מקומי. הדבר מומלץ כאשר נתונים קריטיים נמצאים הן במחשבי לקוח והן בשרתים, ואין התקן אחסון ניתן להסרה עבור כל אחד מהמחשבים. במצב זה, משתמשים מבצעים גיבוי מקומי, ומאחסנים את קבצי הגיבוי שלהם על שרת, ואז יש לבצע גיבוי של השרת.

הגדרת אפשרויות גיבוי

Windows Backup מאפשר לשנות את הגדרות ברירת המחדל עבור כל פעולות הגיבוי והשחזור. הגדרות ברירת מחדל אלו מצויות בכרטיסיות בתיבת הדו-שיח Options (תרשים 12.7). כדי לגשת לתיבת הדו-שיח Options, בחר Options מהתפריט Tools.



תרשים 12.7 הכרטיסיה General שבתיבת **הדו-שיח** Options.

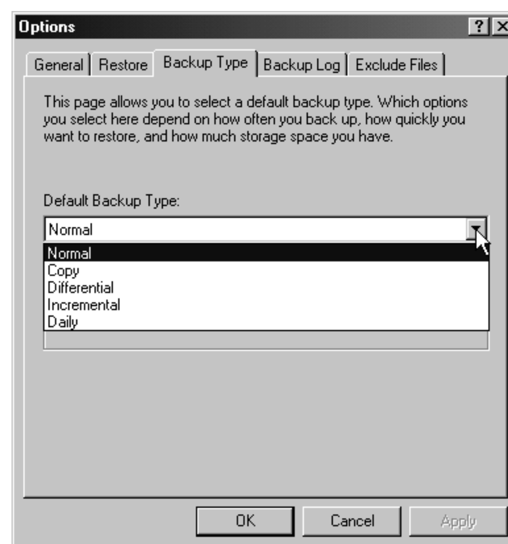
הרשימה להלן מספקת סקירה כללית של הגדרות ברירת המחדל עבור Windows Backup בכרטיסיות שבתיבת הדו-שיח Options:

- **הכרטיסיה General** – ההגדרות משפיעות על אימות נתונים, מידע מצב עבור פעולות גיבוי ושחזור, הודעות אזהרה, ומה מגובה. יש לסמן את תיבת הסימון Verify Data After The Backup Completes, מכיון שחיוני לבדוק שנתוני הגיבוי אינם פגומים.
- **הכרטיסיה Restore** – ההגדרות משפיעות על מה מתרחש, כאשר הקובץ המיועד לשחזור זהה לקובץ קיים.
- **הכרטיסיה Backup Type** – ההגדרות משפיעות על סוג גיבוי ברירת המחדל כאשר מבצעים פעולת גיבוי. האפשרויות שתבחר תלויות בתדירות ביצוע הגיבוי, במהירות השחזור הרצויה ובכמות מקום האחסון המצויה. סוגי גיבוי נדונים ביתר פירוט בהמשך.
- **הכרטיסיה Backup Log** – ההגדרות משפיעות על כמות המידע הנכלל ביומן הגיבוי.
- **הכרטיסיה Exclude Files** – ההגדרות משפיעות על איזה קבצים אינם נכללים בפעולות גיבוי.

ניתן לשנות חלק מהגדרות ברירת המחדל באשף Backup עבור פעולת גיבוי מסוימת. לדוגמה, סוג גיבוי ברירת המחדל הוא Normal (רגיל), אך ניתן לשנות אותו לסוגי גיבוי אחרים באשף הגיבוי. עם זאת, בפעם הבאה שתפעיל את אשף הגיבוי, ייבחר סוג גיבוי ברירת המחדל (Normal).

סוגי גיבוי

Windows Backup מספק חמישה סוגי גיבוי, המגדירים איזה נתונים מגובים: Normal (רגיל), Copy (העתק), Differential (משתנה), Incremental (מצטבר), ו-Daily (יומי). ניתן להגדיר מה סוג ברירת המחדל לגיבוי בכרטיסיה Backup Types, שבתיבת הדו-שיח Options (תרשים 12.8).



תרשים 12.8 הכרטיסיה Backup Types בתיבת הדו-שיח Options.

חלק מסוגי הגיבוי עושה שימוש במאפיין הקובץ (Attribute) בשם Archive (מוכר גם כסיבית ארכיון Archive Bit), המסמן אם הקובץ עבר שינוי. כאשר קובץ משתנה, מופעל המאפיין Archive עבור קובץ זה, המציין שהקובץ השתנה מאז הגיבוי האחרון. סוגי גיבוי מסויימים מאפסים סיבית זו כאינדיקציה לכך שהקובץ עבר גיבוי.

Normal

במהלך גיבוי Normal (רגיל), המוכר כגיבוי מלא (Full Backup), מגובים כל הקבצים והתיקיות שנבחרו. גיבוי רגיל אינו מסתמך על מאפייני הקובץ Archive, לקביעת איזה קבצים לגבות, אולם כן מאפס אותו בכל הקבצים המגובים ומציין על ידי כך שהקובץ עבר גיבוי. גיבויים רגילים מזרזים את הליך השחזור, מכיון שקבצי הגיבוי

הם העדכניים ביותר, ואין צורך לשחזר מספר פעולות גיבוי. עם זאת, הם גם דורשים את הזמן הרב ביותר ואת קיבולת האחסון הגבוהה ביותר ביחס לכל סוג גיבוי אחר.

Copy

במהלך גיבוי Copy (העתק), מגובים כל הקבצים והתיקיות שנבחרו. גיבוי זה אינו מחפש ואינו מאפס את המאפיין Archive. אם לא רוצים לאפס את מאפיין Archive ולהשפיע על סוגי גיבוי אחרים, יש להשתמש בגיבוי זה. לדוגמה, השתמש בגיבוי copy לשכפול נפח נתונים גדול בין מחשבים, מבלי להשפיע על תהליך הגיבוי היומיומי.

Differential

במהלך גיבוי Differential (משתנה), מגובים רק הקבצים והתיקיות שנבחרו, ואשר מאפיין Archive מופעל המציין שהקבצים חדשים או עברו שינוי מאז הגיבוי האחרון. מכיון שגיבוי משתנה (Differential) אינו מאפס את המאפיין Archive, אם ביצעת שני גיבויים משתנים ברצף על קובץ, הקובץ יגובה בכל פעם. סוג גיבוי זה מהיר במידה בינונית לגיבוי ולשחזור נתונים. לביצוע שחזור מלא, תוך שימוש בגיבוי משתנה, יש להשתמש בגיבוי הרגיל (המלא) האחרון ולאחריו הגיבוי המשתנה האחרון.

Incremental

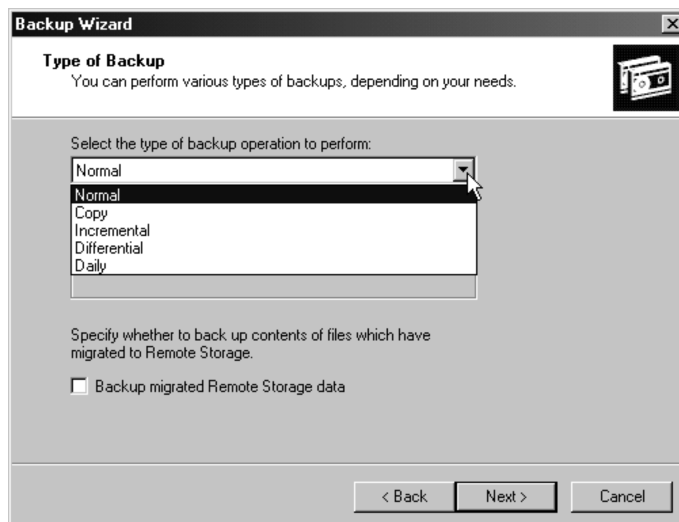
במהלך גיבוי Incremental (מצטבר), מגובים רק קבצים ותיקיות שנבחרו, ושבהם המאפיין Archive מופעל. גיבוי מצטבר מאפס את המאפיין Archive ומציין שהקובץ עבר גיבוי. מכיון שהוא מאפס את המאפיין Archive, אם ביצעת שני גיבויים מצטברים ברצף על קובץ ולא השתנה דבר בקובץ, אז הקובץ לא יגובה בפעם השנייה. סוג גיבוי זה מהיר מאוד בגיבוי נתונים ואיטי בשחזור נתונים. לביצוע שחזור מלא בעזרת גיבוי מצטבר, יש להשתמש תחילה בגיבוי הרגיל (המלא) האחרון, ולאחריו כל אחד מהגיבויים המצטברים לפי הסדר עד לאחרון שבהם.

Daily

בגיבוי Daily (יומי), כל הקבצים והתיקיות שנבחרו ואשר השתנו במהלך היום מגובים. גיבוי יומי אינו מחפש ואינו מאפס את המאפיין Archive. אם רוצים לגבות את כל הקבצים והתיקיות המשתנים לאורך היום מבלי להשפיע על תזמון גיבוי כלשהו, ניתן להשתמש בגיבוי יומי.

הגדרת סוגי גיבוי עבור פעולות מסוימות

ניתן להגדיר את סוג הגיבוי עבור פעולת גיבוי מסוימת, כאשר מפעילים את אשף Backup (תרשים 12.9). אשף הגיבוי מתואר בהמשך שיעור זה.



תרשים 12.9 הגדרת סוג הגיבוי עבור פעולת גיבוי מסוימת.

ניתן גם להגדיר את סוג הגיבוי עבור פעולת גיבוי מסוימת, כאשר מבצעים גיבוי ללא אשף הגיבוי. בכרטיסיה Backup של היישום Windows Backup, לחץ על Start Backup. במסך Backup Job Information המוצג לאחר תחילת הליך הגיבוי, לחץ על Advanced. כאשר מוצגת תיבת הדו-שיח Advanced Backup Options, בחר את סוג הגיבוי מהרשימה הנפתחת.

שילוב סוגי גיבוי

אסטרטגיית גיבוי יעילה עשויה לשלב מספר סוגי גיבוי שונים. חלק מסוגי הגיבוי דורשים יותר זמן לגיבוי הנתונים, אך פחות זמן לשחזורם. לעומת זאת, סוגי גיבוי אחרים דורשים פחות זמן לגיבוי הנתונים, אולם יותר זמן לשחזורם. אם משלבים סוגי גיבוי, ההתייחסות למאפיין Archive היא קריטית. סוגי גיבוי מצטבר ומשתנה בודקים ומסתמכים על מאפיין זה.

המידע להלן מספק דוגמאות לשילוב סוגי גיבוי שונים:

- **גיבויים רגילים ומשתנים** - ביום ראשון מבוצע גיבוי רגיל, ובימים שני עד חמישי מבוצעים גיבויים משתנים. גיבויים משתנים אינם מאפסים את המאפיין Archive של הקבצים, ופירוש הדבר שכל גיבוי כולל את כל השינויים מאז יום שני. אם נתונים נפגמים ביום חמישי, צריך לשחזר רק את הגיבוי הרגיל מיום ראשון ואת הגיבוי המשתנה מיום רביעי. אסטרטגיה זו דורשת זמן רב יותר לגיבוי (לעומת גיבוי מצטבר) אולם פחות זמן לשחזור.
- **גיבויים רגילים ומצטברים** - ביום ראשון מבוצע גיבוי רגיל, ובימים שני עד חמישי מבצעים גיבויים מצטברים. גיבויים מצטברים מאפסים את המאפיין Archive של הקבצים, ופירוש הדבר שכל גיבוי כולל רק את הקבצים שהשתנו מאז הגיבוי הקודם. אם נתונים נפגמים ביום חמישי, יש לשחזר את הגיבוי הרגיל מיום ראשון ואת כל הגיבויים המצטברים מיום שני ועד חמישי. אסטרטגיה זו דורשת פחות זמן לגיבוי אולם יותר זמן לשחזור.
- **גיבויים רגילים, משתנים והעתק** – גיבויים אלה משתמשים באותה אסטרטגיה כמו גיבויים רגילים ומשתנים, אלא שביום שלישי מבצעים גיבוי העתק. גיבויי העתק כוללים את כל הקבצים שנבחרו ואינם מאפסים את המאפיין Archive של הקבצים או מפריעים לתזמון הגיבוי המקובל. לכן, כל גיבוי משתנה כולל את כל השינויים מאז יום ראשון. סוג הגיבוי העתק (Copy) אשר מבוצע ביום שלישי אינו חלק מהשחזור של יום חמישי. גיבויי העתק שימושיים ליצירת תמונה רגעית של הנתונים, בלי להפריע לגיבויים המתוכננים.

גיבוי נתונים

לאחר תכנון הגיבוי, כולל תכנון סוג הגיבוי לשימוש ומתי לבצע פעולות גיבוי, השלב הבא הוא הכנה לגיבוי הנתונים. יש לבצע מספר משימות מקדימות לפני שניתן לגבות את הנתונים. לאחר השלמת המשימות המקדימות, ניתן לבצע את הגיבוי.

ביצוע משימות מקדימות

משימה אחת שיש לבצע לפני כל פעולת גיבוי היא להבטיח שהקבצים הרצויים לגיבוי סגורים. יש לשלוח למשתמשים הודעה לסגור קבצים, לפני שמתחילים בגיבוי נתונים. Windows Backup אינו מגבה קבצים הנעולים במצב פתוח על ידי יישומים. ניתן להשתמש בדואר אלקטרוני, או בתיבת הדו-שיח Send Console Message בתוסף התוכנה File Service Management, לשליחת הודעות מנהלתיות למשתמשים. ניתן לגשת לתוסף התוכנה File Service Management דרך תוסף התוכנה Computer Management.

הערה תוכניות גיבוי רבות מגורם שלישי מסוגלות ליצור גיבויי דמות (Image Backups) של קבצים פתוחים.

אם משתמשים בהתקן אחסון ניתן להסרה, יש לוודא את הפריטים הבאים:

❖ התקן הגיבוי מחובר למחשב ברשת ומופעל. אם מגבים לטייפ, יש לחבר את התקן הטייפ למחשב שעליו מפעילים את Windows Backup.

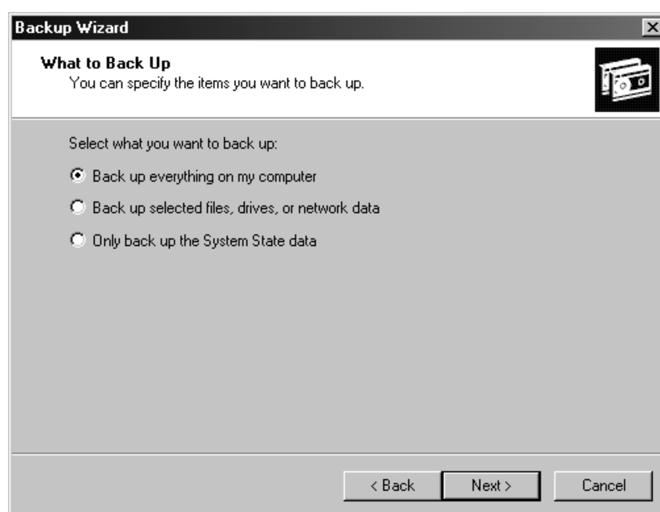
❖ התקן האחסון רשום ברשימת Windows 2000 HCL.

❖ האמצעי הדרוש טעון בהתקן. לדוגמה, אם משתמשים בכונן טייפ, יש לוודא שיש טייפ טעון בתוך הכונן.

בחירת קבצים ותיקיות לגיבוי

לאחר סיום המשימות המקדימות, ניתן לבצע את הגיבוי באמצעות אשף הגיבוי. להפעלת אשף הגיבוי, פתח את Backup, ולחץ על לחצן Backup Wizard בכרטיסייה Welcome.

השלב הראשון בהגדרת גיבוי הוא בחירת הנתונים הרצויים לגיבוי (תרשים 12.10).



תרשים 12.10 מסך What To Backup באשף Backup.

יש לבחור אחת מהאפשרויות הבאות:

- ❖ **Back up everything on my computer** – מגבה את כל הקבצים על המחשב שממנו מפעילים את Windows Backup, מלבד אותם קבצים ש- Windows Backup אינו כולל כברירת מחדל, כגון קבצי ניהול הספק מסוימים.
- ❖ **Back up selected files, drives, or network data** – מגבה קבצים ותיקיות שנבחרו. הדבר כולל קבצים ותיקיות במחשב שממנו מפעילים את Windows Backup, וכל קובץ או תיקיה משותפים ברשת. כאשר לוחצים על אפשרות זו, אשף הגיבוי מציג תצוגה היררכית של המחשב והרשת (באמצעות My Network Places).
- ❖ **Only back up the system state data** – מגבה את מחסן Active Directory, הרישום, התיקיה SYSVOL, מסד הנתונים COM+ Class Registration, קבצי מערכת ההפעלה, ואת Certificate Services (אם מותקנים). Active Directory store והתיקיה SYSVOL זמינים רק ב-DC. השתמש באפשרות זו ליצירת עותק של מחסן Active Directory, המכיל את כל האובייקטים ב-domain ואת המאפיינים שלהם. יש לעצור את Certificate Services לפני גיבוי אפשרות זו. Windows Backup ייכשל אם קיימים Certificate Services פעילים במערכת. יש לשמור את קובץ גיבוי Certificate Services שנוצר על ידי גיבוי Certificate Services עם הגיבוי. כל נתוני מצב המערכת הרלוונטיים למחשב שלך מגובים או משוחזרים יחד. לא ניתן לגבות או לשחזר רכיבים נפרדים של נתוני מצב המערכת (System State Data), בגלל התלות ההדדית בין רכיבים אלה.

בחירת יעד גיבוי והגדרות אמצעי אחסון

לאחר בחירת הנתונים שרוצים לגבות, יש לספק מידע אודות אמצעי הגיבוי. הטבלה הבאה מתארת את המידע שיש לספק עבור אפשרויות אמצעי הגיבוי:

אפשרות	תיאור
Backup Media Type	אמצעי האחסון שבשימוש, כגון טייפ או קובץ. קובץ יכול להיות ממוקם על כל אמצעי מבוסס דיסק, כולל דיסק קשיח, תיקיית רשת משותפת, או דיסק הניתן להסרה, כגון כונן Iomega Zip.
Backup Media Or File Name	המיקום בו Windows Backup יאחסן את הנתונים. עבור טייפ, הזן את שם הטייפ. עבור קובץ, הזן את הנתיב עבור קובץ הגיבוי.

לאחר אספקת מידע אודות אמצעי האחסון, אשף הגיבוי מציג את הגדרות האשף ואת היכולת לבצע אחת משתי האפשרויות הבאות:

- ❖ **Start the Backup** – אם לוחצים Finish, מתחיל הליך הגיבוי, ואשף הגיבוי מציג מידע מצב אודות פעולת הגיבוי בתיבת הדו-שיח Backup Progress.
- ❖ **Specify advanced backup options** – אם לוחצים Advanced, אשף הגיבוי מאפשר לבחור הגדרות גיבוי מתקדמות. הגדרות הגיבוי המתקדמות מתוארות בסעיף הבא.

הערה בתוך הליך הגיבוי, ניתן לבחור לסקור את דוח הגיבוי, שהוא יומן הגיבוי. **יומן גיבוי** הוא קובץ טקסט הרושם פעולות גיבוי ומאוחסן על הדיסק הקשיח של המחשב שממנו מפעילים את Windows Backup.

הגדרות גיבוי מתקדמות

כאשר בוחרים הגדרות גיבוי מתקדמות, משנים את הגדרות ברירת המחדל לגיבוי עבור פעולת הגיבוי הנוכחית בלבד.

הטבלה שלהלן מתארת את האפשרויות המתקדמות הניתנות להגדרה.

אפשרות מתקדמת	תיאור
Select The Type of Backup Operation To Perform	מאפשר לבחור את סוג הגיבוי עבור פעולת גיבוי זו. בחר אחת מהאפשרויות הבאות: Normal, Copy, Incremental, Differential או Daily.
Backup Migrated Remote Storage Data	מגבה נתונים ש- HSM (**H**ierarchical **S**torage **M**anager) העביר לאחסון מרוחק.
Verify Data After Backup	מוודא שהקבצים מגובים נכון. Windows Backup משווה את נתוני הגיבוי עם נתוני המקור, כדי לוודא שהם זהים. Microsoft ממליצה לבחור באפשרות זו.
Use Hardware Compression, If Available	מאפשר דחיסת נתונים ברמת חומרה עבור התקני טייפ התומכים בה. אם התקן הטייפ אינו תומך בדחיסה, האפשרות אינה זמינה.
If The Archive Media Already Contains Backups	מציין האם להוסיף לסוף או להחליף את הגיבוי הקיים על אמצעי האחסון. בחר Append, כדי לאחסן מספר עותקי גיבוי בהתקן אחסון יחיד, או בחר Replace, אם אין צורך לשמור פעולות גיבוי קודמות, ורוצים לשמור רק את נתוני הגיבוי העדכני ביותר.

אפשרות מתקדמת	תיאור
Allow Only The Owner And The Administrator Access To The Backup Data And To Any Backups Appended To The Media	מאפשר להגביל את הגישה של אנשים אל קובץ או טייפ הגיבוי בתום גיבוי. אפשרות זו זמינה רק אם בוחרים להחליף גיבוי קיים באמצעי אחסון, ולא להוסיף את הגיבוי לאחר הגיבוי הקיים. אם מגבים את הרישום (Registry) או את מחסן Active Directory, יש לבחור אפשרות זו, כדי למנוע מאנשים אחרים לקבל עותקים של פעולת הגיבוי.
Backup Label	מאפשר לציין שם ותיאור עבור פעולת הגיבוי. השם והתיאור מוצגים ביומן הגיבוי. ניתן לשנות את השם והתיאור לשם אינטואיטיבי יותר (לדוגמה - Sales - normal backup September 27, 2000.
Media Label	מאפשר לציין שם עבור אמצעי האחסון (לדוגמה, שם הטייפ). בפעם הראשונה שמגבים לאמצעי חדש, או כותבים מעל פעולת גיבוי קיימת, ניתן לציין את השם, כגון Active Directory store backup (גיבוי מחסן Active Directory).
When To Back Up	מאפשר לציין Now או Later. אם בוחרים מאוחר יותר, יש לציין את שם הפעולה ואת תאריך ההתחלה. ניתן גם להגדיר את התזמון.

בהתאם לבחירה האם לגבות עתה או מאוחר יותר, אשף הגיבוי יספק את היכולת לבצע אחת מהפעולות הבאות:

- ❖ אם בוחרים לסיים את הליך הגיבוי, אשף הגיבוי מציג את הגדרות Completing The Backup Wizard, ואז מציג את האפשרות לסיים ולהתחיל מייד בגיבוי. במהלך הגיבוי, האשף מציג מידע מצב אודות פעולת הגיבוי.
- ❖ אם בוחרים לגבות מאוחר יותר, מוצגות תיבות דו-שיח נוספות, בהן מתזמנים את הליך הגיבוי שיתרחש מאוחר יותר, כמתואר בסעיף הבא.

תזמון פעולות גיבוי

תזמון פעולת גיבוי מאפשר לגרום לפעולת גיבוי להתבצע ללא השגחה במועד מאוחר יותר, כמו למשל, כאשר משתמשים אינם בעבודה והקבצים סגורים. ניתן גם לתזמן פעולות גיבוי שיתרחשו בזמנים קצובים. Windows 2000 תומכת ביכולת תזמון זו, על ידי שילוב Windows Backup עם השירות Task Scheduler (מתזמן משימות).

לתזמון גיבוי, לחץ על לחצן האפשרות Later במסך When To Back Up באשף הגיבוי. Task Scheduler מציג את תיבת הדו-שיח Set Account Information, המבקשת ממך סיסמה. לחשבון המשתמש צריכות להיות הרשאות משתמש מתאימות לביצוע פעולות גיבוי.

הערה אם שירות Task Scheduler **אינו פעיל או שאינו מוגדר לפעול אוטומטית,** Windows 2000 **תציג תיבת דו-שיח המבקשת להפעיל את השירות. לחץ** OK, **ותוצג תיבת הדו-שיח** Set Account Information.

בתיבת הדו-שיח Schedule Job, ניתן להגדיר את התאריך, השעה, ואת מספר המופעים שבהם תחזור פעולת הגיבוי, כמו למשל, כל יום שישי בשעה 10:00 PM. ניתן גם להציג את כל הפעילויות המתוזמנות עבור המחשב, על ידי סימון תיבת הסימון Show Multiple Schedules. הדבר מסייע למניעת תזמון מספר פעולות על אותו מחשב באותו זמן.

על ידי לחיצה על הלחצן Advanced, ניתן גם לתזמן מה יהיה אורך הגיבוי, ולמשך כמה ימים, שבועות, חודשים, או שנים רוצים להמשיך בתזמון זה.

לאחר תזמון פעולת הגיבוי והשלמת אשף הגיבוי, Windows Backup מציב את פעולת הגיבוי בלוח השנה בכרטיסיה Schedule Jobs ב-Windows Backup. פעולת הגיבוי תופעל אוטומטית במועד שנבחר.

טיפ אם המחשב **המיועד לגיבוי מפעיל** Certificate Services, **ניתן לתזמן את** Certificate Services **שיפסיק לפני תחילת הגיבוי. בסיום הגיבוי, ניתן לתזמן את** Task Scheduler **שיפעיל מחדש את** Certificate Services. **הדרך הקלה ביותר לביצוע פעולות אלו היא להפסיק ולהפעיל את** Certificate Services, **וליזום את פעולת הגיבוי מתוך קובץ פקודה יחיד. אז מתזמנים את קובץ הפקודה לפעול באמצעות** Task Scheduler. **תהליך זה מתואר לקראת סיום תרגיל 1 בפרק זה.**

תרגיל 1: גיבוי קבצים

בתרגיל זה תשתמש באשף הגיבוי לגיבוי מספר קבצים אל הדיסק הקשיח. אז תיצור פעולת גיבוי שתבצע גיבוי במועד מאוחר יותר על ידי שימוש ב- Task Scheduler. בצע תרגיל זה על Server01.

הליך 1: יצירה, הפעלה ואימות פעולת גיבוי

בהליך זה, תפעיל את Windows Backup, ותשתמש באשף הגיבוי לגיבוי קבצים אל הדיסק המקומי ב-Server01.

1. היכנס ל-Server01 בשם משתמש Administrator עם הסיסמה password.
2. לחץ Start, ולחץ Run. תופיע תיבת הדו-שיח Run.
3. בתיבת הטקסט Open, הקלד **ntbackup** ולחץ OK. תופיע תיבת הדו-שיח Backup - [Untitled].
4. קרא את התיאורים המוצגים עבור שלוש האפשרויות בכרטיסיה Welcome, ולחץ על Backup Wizard.

   אשף הגיבוי יופעל ויציג את המסך Welcome To The Windows 2000 Backup And Recovery Tools.
5. לחץ Next. יופיע מסך What To Back Up, בו יש לבחור את היקף פעולת הגיבוי.
6. לחץ על לחצן האפשרות Back Up Selected Files, Drives, Or Network Data, ולחץ Next. יופיע המסך Items To Back Up, בו יש לבחור את הכוננים המקומיים וכונני הרשת, התיקיות, והקבצים הרצויים לגיבוי.
7. הרחב את My Computer.
8. לחץ פעם אחת על המילים System State (אל תסמן את תיבת הסימון משמאל ל-System State).

   שים לב שבחלונית הפרטים, מגובים הפרטים הבאים: Active Directory store, קבצי Boot, הגדרות Registry, מסד נתונים COM+ Class Registration, התיקיה SYSVOL, ומסד נתונים Certificate Services.
9. בחלונית השמאלית, הרחב את :C ולחץ על האות C. אל תסמן את תיבת הסימון משמאל ל- :C.

10. בחלונית הפרטים, גלול מטה וסמן את תיבת הסימון Boot.ini ולחץ Next. יופיע המסך Where To Store The Backup.

הערה אם לא מחובר כונן טייפ כלשהו אל המחשב, תיבת הרשימה הנפתחת Backup Media Type תהיה אפורה, מכיון שסוג אמצעי הגיבוי היחיד הזמין יהיה File.

---

11. בתיבת הטקסט Backup Media Or File Name, הקלד **C:\backup1.bkf** ולחץ Next.

הערה בדרך כלל מגבים לטייפ, לקובץ המאוחסן בדיסק קשיח אחר, לדיסקים ניתנים להסרה (כגון כונני Iomega Zip ו- Jaz), לתקליטורים המאפשרים הקלטה, או לכוננים אופטיים. אולם, למען הפשטות, הגיבוי כאן מבוצע לאותו כונן עליו נמצא הקובץ.

המסך Completing The Backup Wizard יופיע, יראה את פרטי פעולת הגיבוי המתבצעת ויאפשר לבחור בין המשך לבין הגדרות נוספות לפעולת גיבוי זו.

12. לחץ Advanced, כדי לציין אפשרויות גיבוי נוספות. יופיע המסך Type Of Backup.

13. התבונן בסוגי הגיבוי המוצגים בתיבת הרשימה הנפתחת Select The Type Of Backup Operation To Perform. סוגי גיבוי אלה תוארו לעיל לפני תרגיל זה.

14. ודא שנבחר Normal.

15. ודא שתיבת הסימון Backup Migrated Remote Storage Data ריקה.

אפשרות זו תומכת בתכונות HSM ב- Windows 2000 Server.

16. לחץ Next. יופיע המסך How To Backup, המבקש לציין האם לאמת את נתוני הגיבוי בתום פעולת הגיבוי, או לא.

17. סמן את תיבת הסימון Verify Data After Backup, ולחץ Next.

יופיע הדף Media Options, המבקש לציין האם להוסיף פעולת גיבוי זו לאמצעי גיבוי קיים או לכתוב מעל נתוני גיבוי קיימים באמצעי היעד.

18. לחץ על לחצן האפשרות Replace The Data On The Media With This Backup.

שים לב לתיבת הסימון Allow Only The Owner And The Administrator Access To The Backup Data And Any Backups Appended To This Media. אפשרות זו מספקת אבטחה רבה יותר, כיון שכאשר היא נבחרת, רק בעל הגיבוי והמנהל יכולים לשחזר פעולת גיבוי. ודא שאפשרות זו לא נבחרה.

19. לחץ Next. יופיע המסך Backup Label, המבקש לספק תווית עבור פעולת הגיבוי ועבור אמצעי הגיבוי.

שים לב ש- Windows Backup מייצר תווית גיבוי ותווית אמצעי גיבוי על ידי שימוש בתאריך ובשעה הנוכחיים.

20. בתיבת הטקסט Backup Label, הקלד **Boot.ini backup set created on <date>** (כאשר <date> הוא התאריך והשעה הנוכחיים).

21. השאר את תיבת הטקסט Media Label ללא שינוי, ולחץ Next.

יופיע המסך When To Back Up, בו יש לבחור האם להפעיל את פעולת הגיבוי כעת, או לתזמן אותה למועד אחר.

22. ודא שלחצן האפשרות Now נבחר, ולחץ Next. יוצג המסך Completing The Backup Wizard.

23. לחץ Finish להתחלה של פעולת הגיבוי.

Windows Backup יציג לזמן קצר את תיבת הדו-שיח Selection Information, המציינת את כמות הנתונים ואת הזמן הנדרש להשלמה של פעולת הגיבוי.

אז Windows Backup יציג את תיבת הדו-שיח Backup Progress, המציגה את מצב פעולת הגיבוי, סטטיסטיקה לגבי כמות מוערכת וכמות בפועל של נתונים מעובדים, את הזמן שעבר, והערכה לכמות הזמן שנותרה לביצוע פעולת הגיבוי.

24. כאשר תיבת הדו-שיח Backup Progress מציגה שפעולת הגיבוי הסתיימה, לחץ על הלחצן Report. תופעל התוכנה Notepad ובה יוצג דוח הגיבוי.

דוח הגיבוי מכיל נתוני מפתח אודות פעולת הגיבוי, כגון שעת ההתחלה וכמה קבצים נכללו.

25. קרא את הדוח, ובסיום סגור את Notepad.

26. בתיבת הדו-שיח Backup Progress, לחץ Close.

תוצג תיבת הדו-שיח Backup - [Untitled] בה הכרטיסיה Welcome פעילה.

הליך 2: יצירה, הפעלה ואימות פעולת גיבוי מתוזמנות

בהליך זה, תיצור פעולת גיבוי, שתבצע גיבוי במועד מאוחר יותר באמצעות Task Scheduler.

1. בכרטיסיה Welcome, לחץ על Backup Wizard.

   Backup Wizard יתחיל לפעול, ויציג את המסך Welcome To The Windows 2000 Backup And Recovery Tools.

2. לחץ Next. יופיע מסך What To Back Up, שבו יש לבחור את היקף פעולת הגיבוי.
3. לחץ על לחצן האפשרות Back Up Selected Files, Drives, Or Network Data, ולחץ Next. יופיע המסך Items To Back Up, שבו יש לבחור את הכוננים המקומיים וכונני הרשת, התיקיות והקבצים הרצויים לגיבוי.
4. הרחב את My Computer, הרחב את כונן C, ואז סמן את תיבת הסימון Inetpub.
5. לחץ Next. יופיע המסך Where To Store The Backup, בו יש לבחור את היעד עבור הגיבוי.
6. בתיבת הטקסט Backup Media Or File Name, הקלד **C:\backup2.bkf** ולחץ Next. יופיע המסך Completing The Backup Wizard.
7. לחץ על הלחצן Advanced, כדי לציין אפשרויות גיבוי נוספות. יופיע המסך Type Of Backup, בו יש לבחור סוג גיבוי עבור פעולת גיבוי זו.
8. בתיבת הרשימה הנפתחת Type Of Backup Operation To Perform, ודא שנבחר Normal.
9. לחץ Next. יופיע המסך How To Backup, המבקש לציין האם לאמת את נתוני הגיבוי בתום פעולת הגיבוי, או לא.
10. סמן את תיבת הסימון Verify Data After Backup, ולחץ Next. יופיע המסך Media Options, המבקש לציין האם להוסיף פעולת גיבוי זו לאמצעי גיבוי קיים, או לכתוב מעל נתוני גיבוי קיים באמצעי היעד.
11. לחץ על לחצן האפשרות Replace The Data On The Media With This Backup.
12. ודא שתיבת הסימון Allow Only The Owner And The Administrator Access To The Backup Data And Any Backups Appended To This Media אינה מסומנת, ולחץ Next. יופיע המסך Backup Label, המבקש לספק תווית עבור פעולת הגיבוי ועבור אמצעי הגיבוי.
13. בתיבת הטקסט Backup Label, הקלד **Inetpub backup set created on <date>** (כאשר <date> הוא התאריך והשעה הנוכחיים).

14. השאר את תיבת הטקסט Media Label ללא שינוי, ולחץ Next. יופיע המסך When To Back Up, שבו יש לבחור האם להפעיל את פעולת הגיבוי כעת, או לתזמן אותה למועד אחר.

15. לחץ על לחצן האפשרות Later.

תופיע תיבת הדו-שיח Set Account Information, שבה יש להקליד את הסיסמה עבור חשבון MICROSOFT\administrator. (אם השירות Task Scheduler אינו מוגדר להתחיל אוטומטית, ייתכן שתראה תחילה תיבת דו-שיח שבה שאלה, האם ברצונך להפעיל את Task Scheduler. לחץ OK, ואז תופיע תיבת הדו-שיח Set Account Information).

כיון שהשירות Task Scheduler מפעיל אוטומטית יישומים בתוך הקשר האבטחה של משתמש תקף עבור המחשב או ה-domain, תתבקש להקליד שם וסיסמה שאיתם תופעל הפעולה המתוזמנת. עבור פעולות גיבוי מתוזמנות, יש לספק חשבון משתמש, שהוא חבר בקבוצה Backup Operators עם הרשאות גישה לכל התיקיות והקבצים המיועדים לגיבוי.

למען הפשטות, תשתמש בחשבון Administrator להפעלת פעולת הגיבוי המתוזמנת.

16. ודא שמוצג MICROSOFT\administrator בתיבת הטקסט Run As, ואז בתיבות הטקסט Password ו- Confirm Password הקלד **password**.

17. לחץ OK.

18. בתיבת הטקסט Job Name, הקלד **Inetpub Backup**, ולחץ Set Schedule.

19. בתיבת הרשימה הנפתחת Schedule Task בחר Daily Is Selected, ובתיבה Start Time הזן שעה בעוד 5 דקות מהשעה הנוכחית.

20. לחץ Advanced. תוצג תיבת הדו-שיח Advanced Schedule Options.

21. סמן את תיבת הסימון End Date, ומתיבת הרשימה הנפתחת בחר את התאריך של מחר, ולחץ OK. תופיע תיבת הדו-שיח Schedule Job.

22. לחץ OK. יופיע המסך When To Backup.

23. לחץ Next. יופיע המסך Completing The Backup Wizard, ובו מוצגות האפשרויות וההגדרות שבחרת עבור פעולת גיבוי זו.

24. לחץ Finish להתחלת פעולת הגיבוי. תוצג תיבת הדו-שיח Backup - [Untitled], בה הכרטיסיה Welcome פעילה.

25. סגור את תיבת הדו-שיח Backup - [Untitled]. כאשר מגיע הזמן להתחלת פעולת הגיבוי, Windows Backup יתחיל לבצע את פעולת הגיבוי המבוקשת.

26. הפעל את Windows Explorer, לחץ על כונן C וודא ש- Backup2.bkf קיים.

הליך 3: הצגה והגדרה של משימות

בהליך זה, תעיין במשימת הגיבוי המתוזמנת, ותיצור משימה חדשה.

1. לחץ Start, הצבע על Programs, הצבע על Accessories, הצבע על System Tools, ולחץ על Scheduled Tasks. יופיע החלון Scheduled Tasks.

   שים לב שמופיעה המשימה Inetpub Backup.

2. לחץ לחיצה כפולה על Inetpub Backup. תופיע תיבת הדו-שיח Inetpub Backup.

   שים לב לטקסט בתיבת הטקסט Run. זוהי הפקודה ntbackup עם הפרמטרים שנוצרו על ידי אשף Backup לגיבוי Inetpub.

   אם יש צורך לעצור שירות, כגון Certificate Services, לפני הפעלת פעולת גיבוי, ניתן ליצור קובץ אצווה (cmd או bat) העוצר את השירות, מפעיל את פעולת הגיבוי, ואז מפעיל מחדש את השירות. הפקודה להפסקת Certificate Services היא:

net stop “certificate services”

   הפקודה להפעלה מחדש של Certificate Services היא:

net start “certificate services”

3. בחר בכרטיסיה Schedule. שים לב שזה התזמון שיצרת באמצעות האשף Backup.

4. לחץ OK לסגירת תיבת הדו-שיח Inetpub Backup. יוצג החלון Scheduled Tasks.

5. פתח את תפריט File, ולחץ Delete. תוצג תיבת ההודעה Confirm File Delete בה שאלה האם למחוק את המשימה המתוזמנת.

6. לחץ Yes.

7. סגור את החלון Scheduled Tasks.

סיכום שיעור

Windows Backup הוא כלי המאפשר גיבוי ושחזור נתונים בקלות. ניתן להשתמש ב-Windows Backup לגיבוי נתונים ידנית, או לתזמון פעולות גיבוי ללא השגחה באופן סדיר. יש לתכנן את פעולות הגיבוי כך שיתאימו לצרכי החברה. Windows Backup מאפשר לשנות את הגדרות ברירת המחדל עבור כל פעולות הגיבוי והשחזור. הוא מספק חמישה סוגי גיבוי המגדירים איזה מידע מגובה: רגיל, העתקה, משתנה, מצטבר ויומי. לפני גיבוי נתונים, יש לוודא שכל הקבצים המיועדים לגיבוי סגורים, ובמידת הצורך יש להכין את אמצעי הגיבוי הניתנים להסרה. לאחר השלמת המשימות המקדימות, ניתן לבצע את הגיבוי באמצעות אשף Backup. אשף Backup מאפשר לבחור את הקבצים והתיקיות לגיבוי, ולציין את יעד הגיבוי ואת הגדרות אמצעי הגיבוי. האשף גם מאפשר לציין הגדרות מתקדמות עבור פעולת הגיבוי הנוכחית ולתזמן פעולות גיבוי.

שיעור 3: יישום הגנה מפני אסון

אסון מחשב הוא אירוע כלשהו הגורם למחשב לא להיות מסוגל לאתחל. הדבר יכול לכלול הרס רשומת האתחול העיקרית (**M**aster **B**oot **R**ecord - MBR) המאוחסנת בהתקן מערכת, מחיקת קובץ מערכת הפעלה אחד או יותר, הרס התקן המערכת הפיסי של המחשב, או הרס המחשב עצמו. המונח **הגנה מפני אסון** (Disaster protection) מתייחס למאמץ כלשהו למניעת אסונות מחשב, ולהפחתת זמן ההשבתה במקרה של כשל מערכת. ניתן להגיע לרמה כלשהי של הגנה מפני אסון על ידי שימוש במכשיר אל-פסק (**U**ninterruptible **P**ower **S**upply - UPS) ויישום סיבולת לתקלות (Fault tolerance) באמצעות מערכי יתירות דיסק (RAID).

לאחר שיעור זה, תוכל

- להגדיר UPS לאספקת מתח, למקרה של הפסקת חשמל מקומית.
- ליישם fault tolerance על דיסק.

זמן לימוד משוער: 40 דקות

הגדרת אל-פסק (UPS)

התאוששות מאסון היא שחזור מחשב, כך שניתן להיכנס ולגשת למשאבי מערכת לאחר התרחשות אסון מחשב. סוג נפוץ אחד של אסון מחשב הוא הפסקת חשמל מקומית, שעלולה לגרום לאובדן או נזק לנתונים על מחשב שרת או לקוח. בעוד שחברות מגינות בדרך כלל על שרתים נגד אסון מסוג זה, כדאי לשקול גם אספקת הגנה למחשבי לקוח נגד הפסקות חשמל, בהתאם לאמינות אספקת החשמל המקומית.

אל-פסק (**U**ninterruptible **P**ower **S**upply - UPS) מספק מתח במקרה של הפסקת חשמל מקומית ומסווג בדרך כלל לאספקת כמות מסוימת של מתח למשך פרק זמן נתון. באופן כללי, UPS צריך לספק מתח לפרק הזמן הנדרש לכיבוי מחשב באופן מסודר על ידי סיום הליכים וסגירת תוכניות.

הערה לפני רכישת UPS לשימוש עם Windows 2000, יש לבדוק האם ההתקן המוצע נמצא ברשימת Windows 2000 HCL.

הגדרת אפשרויות עבור שירות UPS

השתמש בכרטיסיה UPS של תיבת הדו-שיח Power Options Properties (אפשרויות צריכת חשמל) להגדרת שירות UPS. ניתן לגשת לתיבת דו-שיח זו על ידי בחירה ב-Power Options בלוח הבקרה. להגדרת שירות UPS, יש לציין את המידע הבא :

- ❖ יציאת COM אליה מחובר ה-UPS.
- ❖ התנאים הגורמים להתקן UPS לשלוח אות, כגון הפסקת חשמל, מתח מצבר נמוך וכיבוי מרחוק על ידי התקן UPS.
- ❖ מרווח הזמן לשמירת מתח מצבר, טעינת המצבר ושליחת הודעות שגיאה לאחר הפסקת חשמל.

הערה אפשרויות ההגדרה עבור שירות UPS עשויות להשתנות, בהתאם להתקן UPS המסוים המחובר למחשב. לפרטים אודות הגדרות אפשריות, ראה תיעוד היצרן המסופק עם התקן UPS.

בדיקת הגדרות UPS

לאחר הגדרת אפשרויות שירות UPS עבור המחשב, יש לבצע בדיקת מבחן. ניתן לדמות הפסקת חשמל על ידי ניתוק אספקת המתח העיקרית להתקן UPS. במהלך הבדיקה, המחשב וההתקנים ההיקפיים המחוברים להתקן UPS צריכים להישאר פעילים, הודעות צריכות להיות מוצגות, ואירועים צריכים להירשם ביומן.

הערה אין להשתמש במחשב ייעודי לבדיקת הגדרות UPS. יש להשתמש במחשב חליפי או במחשב בדיקה. אם משתמשים במחשב ייעודי, עלולים לאבד חלק מהנתונים במחשב, ואף ייתכן צורך להתקין מחדש את Windows 2000. זכור, כאשר מחשב מפסיק פתאום, ייתכן אובדן או נזק לנתונים. הסיבה לשימוש ב- UPS היא לאפשר למחשבים כיבוי מסודר במקום הפסקה פתאומית.

בנוסף, יש להמתין עד שמצבר ה-UPS מגיע לרמה נמוכה, כדי לוודא התרחשות כיבוי מסודר. אז, החזר את אספקת המתח להתקן UPS, ובדוק ביומן האירועים האם כל הפעולות נרשמו ולא היו שגיאות.

הערה יצרני UPS אחדים מספקים תוכנת UPS עם ההתקן, כדי לנצל את התכונות הייחודיות של התקני UPS שלהם.

Fault Tolerance

סיבולת תקלות (Fault Tolerance) היא היכולת של מחשב או מערכת הפעלה להגיב לאירוע אסון, כגון הפסקת חשמל או כשל חומרה, כך שלא יאבדו נתונים ושלא ייגרם נזק לעבודה המתבצעת. מערכות בעלות Fault tolerance מלאה, המשתמשות במערכי דיסקים ל-Fault tolerance, מונעות אובדן נתונים.

למרות שהנתונים זמינים ועדכניים במערכת בעלת Fault tolerance, עדיין יש לבצע גיבויים להגנת הנתונים על דיסקים קשיחים מפני מחיקות בשוגג, שריפה, גניבה או אסונות אחרים. Fault tolerance של דיסק אינה תחליף לאסטרטגיית גיבוי עם אחסון מחוץ לאתר, שהיא הביטוח הטוב ביותר לשחזור נתונים אבודים או ניזוקים.

אם חווית אובדן דיסק קשיח כתוצאה מכשל חשמלי או מכני, ולא יישמת Fault tolerance, האפשרות היחידה לשחזור נתונים מהכונן שכשל היא החלפת הדיסק הקשיח, ושחזור הנתונים מהגיבוי. עם זאת, אובדן הגישה לנתונים בזמן החלפת הדיסק ושחזור הנתונים, עלולים לגרום לאיבוד זמן וכסף.

Fault tolerance הוא כלי המשמש להמשך פעילות במצב קריסת דיסק יחיד, ובכך מאפשרת המשך עבודה רציף עד לשלב שבו תהיה אפשרות להחליף את הדיסק הפגום.

יישום RAID

כדי לשמור על גישה לנתונים במקרה של אובדן דיסק קשיח יחיד, Windows 2000 Server מספקת יישום תוכנה של טכנולוגיית Fault tolerance, המכונה RAID (**R**edundant **A**rray of **I**ndependent **D**isks, מערך יתיר של דיסקים עצמאיים). RAID מספק Fault tolerance על ידי יישום יתירות נתונים. בשימוש ביתירות נתונים, מחשב כותב נתונים ליותר מאשר דיסק יחיד, פעולה המגינה על הנתונים במקרה של כשל בדיסק קשיח.

ניתן ליישם RAID Fault tolerance כפתרון ברמת תוכנה או ברמת חומרה.

יישומי RAID בתוכנה

Windows 2000 Server תומכת בשני יישומי RAID ברמת תוכנה: RAID-1 Mirrored Volumes ו-RAID-5 Striped Volumes with Parity, המוכרים גם כ-RAID-5 Volumes. עם זאת, ניתן ליצור RAID Volumes חדשים רק על דיסקים דינמיים של Windows 2000.

עם יישומי תוכנה של RAID, אין כל Fault tolerance לאחר כשל של אחד הדיסקים עד לתיקונו. אם מתרחשת תקלה נוספת לפני שחזור הנתונים שאבדו כתוצאה מהתקלה הראשונה, ניתן לשחזר את הנתונים רק על ידי שחזור מגיבוי.

הערה כאשר משדרגים Windows NT 4.0 **אל** Windows 2000, **מערכות** Mirror **או** Strip set with parity **קיימות כלשהן נשמרות.** Windows 2000 **מספקת תמיכה מוגבלת במערכות** Fault tolerance **אלו, ומאפשרת לנהל ולמחוק אותן.**

יישום RAID ברמת חומרה

כפתרון חומרה, ממשק בקר הדיסק מטפל בהגדרה ויצירה מחדש של מידע יתיר. ספקי חומרה אחדים מיישמים הגנת נתונים בעזרת RAID ישירות בחומרה, כמו עם כרטיסי בקר מערך דיסקים. כיון ששיטות אלו ייחודיות לספק ועוקפות את מנהלי ההתקנים של התוכנה בעלי Fault tolerance של מערכת ההפעלה, הם מציעים שיפורים בביצועים ביחס ליישומי RAID ברמת תוכנה. בנוסף, יישומי RAID ברמת חומרה כוללים בדרך כלל תכונות נוספות, כגון תצורות נוספות של RAID בעלי Fault tolerance, החלפה חמה של דיסקים קשיחים פגומים, דיסק חלופי חם מקוון וזיכרון מטמון ייעודי לביצועים משופרים.

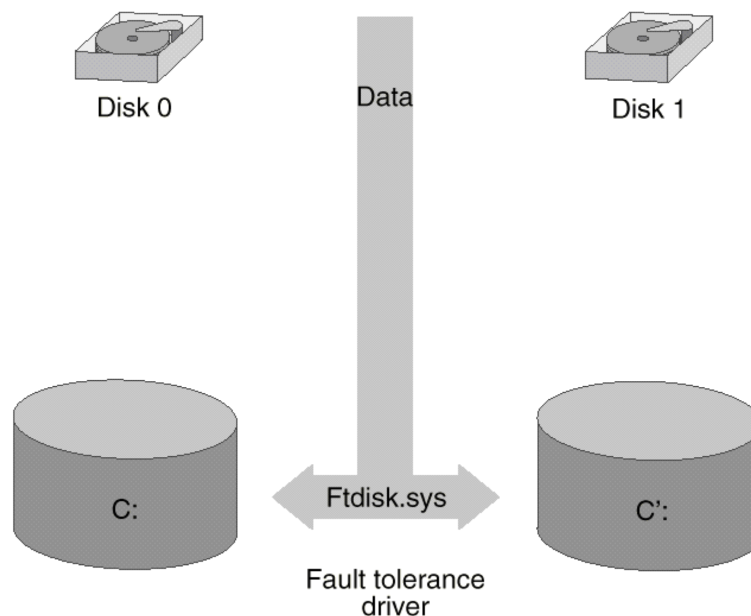
הערה רמת RAID הנתמכת ביישום בחומרה תלויה ביצרן החומרה.

כאשר צריכים לקבל החלטה האם ליישם RAID ברמת חומרה או ברמת תוכנה, יש לשקול את הגורמים הבאים :

- ❖ Fault tolerance בחומרה יקרה יותר מאשר Fault tolerance בתוכנה.
- ❖ Fault tolerance בחומרה מספקת בדרך כלל קלט/פלט דיסק מהיר יותר ביחס ל-Falut tolerance בתוכנה.
- ❖ פתרונות חומרה ל-Fault tolerance עלולים להגביל אפשרויות ציוד לספק יחיד.
- ❖ פתרונות חומרה ל-Fault tolerance עשויים לאפשר החלפה חמה (Hot Swap) של דיסקים קשיחים. כך, ניתן להחליף דיסק פגום ללא כיבוי המחשב (המשמש בדרך כלל כשרת ברשת). בנוסף קיימת גם אפשרות של דיסק חלופי חם מותקן בצורה קבועה (מותקן תמיד ומשמש בעת הצורך בלבד), כך שדיסק פגום מוחלף אוטומטית על ידי דיסק חלופי מקוון.

Mirrored Volumes

Mirrored Volume משתמש ב-Windows 2000 fault Tolerance driver בשם Ftdisk.sys לכתיבת אותם נתונים ל-volume על כל אחד משני דיסקים פיסיים בו-זמנית, כמתואר בתרשים 12.11. כל volume נחשב כחבר ב-Mirrored Volume. יישום Mirrored Volume מסייע להבטחת הישרדות נתונים, במקרה שחבר אחד ב-Mirrored Volume מתקלקל.



תרשים 12.11 Mirrored Volume.

Mirrored Volume יכול להכיל מחיצה (partition) כלשהי, כולל את מחיצת האתחול (Boot Partition) או מחיצת המערכת (System Partition); אולם, שני הדיסקים ב-Mirrored Volume ברמת תוכנה חייבים להיות דיסקים דינמיים של Windows 2000.

Mirrored Volumes המיושמים ברמת חומרה יכולים להיות מפוצלים על פני מספר דיסקים. תצורה זו מכונה במקרים רבים RAID-10. שלא כמו RAID-0, RAID-10 היא תצורת RAID בעלת Fault tolerance, מכיון שכל דיסק בפס גם משוקף. RAID-10 משפר קלט/פלט של דיסק על ידי ביצוע פעולות קריאה וכתיבה בו-זמנית על פני הפס.

ביצועים ב-Mirrored Volumes

Mirrored Volumes יכולים לשפר ביצועי קריאה, כיון ש-Fault Tolerance Driver קורא משני החברים ב-volume בו-זמנית. עשויה להיות ירידה קלה בביצועי הכתיבה, מאחר ש-Fault Tolerance Driver חייב לכתוב את אותם נתונים אל שני החברים. כאשר חבר אחד ב-Mirrored Volume כושל, הביצועים חוזרים למצב הרגיל, כיון ש-Fault Tolerance Driver פועל עם מחיצה (partition) יחידה בלבד.

כיון שניצול שטח הדיסק ביישום Mirrored Volumes הוא רק 50 אחוזים (שני חברים עבור מערכת נתונים יחידה), Mirrored Volumes עשויים להיות יקרים.

אזהרה מחיקת Mirrored Volume תמחק את כל המידע המאוחסן ב-Volume זה.

Disk Duplexing

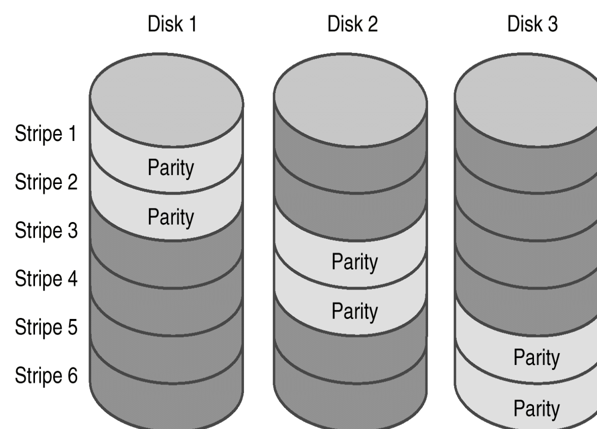
אם בקר דיסק יחיד שולט על שני הדיסקים הפיסיים ב-Mirrored Volume ובקר הדיסק נפגם, אין גישה לאף אחד מחברי ה-Mirrored Volume. ניתן להתקין בקר נוסף במחשב, כך שכל דיסק ב-Mirrored Volume יפעל עם בקר עצמאי שלו. הסדר זה, הנקרא **שכפול דיסק** (Disk Duplexnig), יכול להגן על ה-Mirrored Volume נגד כשל בדיסק וגם נגד כשל בבקר. יישומי חומרה אחדים של שכפול דיסק משתמשים בשני ערוצים או יותר על כרטיס בקר דיסק יחיד.

שכפול דיסק מפחית את תעבורת האפיק ועשוי לשפר את ביצועי הקריאה. שכפול דיסק הוא שיפור חומרה ל-Windows 2000 Mirrored Volume, ואינו דורש הגדרות תוכנה נוספות כלשהן.

RAID-5 Volumes

Windows 2000 Server גם תומכת ב-Fault tolerance, באמצעות RAID-5 - Striped Volumes With Parity. **זוגיות** (Parity) היא שיטה מתמטית לקביעת מספר הסיביות האי-זוגיות והזוגיות במספר או בסדרת מספרים, וניתן להשתמש בזוגיות לשחזור נתונים, אם אחד מהמספרים ברצף מספרים נפגם או אובד.

ב-RAID-5 Volume, Windows 2000 משיגה Fault tolerance על ידי הוספת **פס נתונים זוגי** (Parity Information Stripe) לכל מחיצת דיסק ב-Volume, כמתואר בתרשים 12.12. אם דיסק יחיד כושל, Windows 2000 יכולה להשתמש בנתונים ובמידע הזוגיות בדיסקים הנותרים לשחזור הנתונים שהיו בדיסק שכשל.



תרשים 12.12 פסי נתונים זוגיים ב- RAID-5 (Raid-5 Parity Information Stripes).

בגלל חישובי הזוגיות, פעולות כתיבה ב-RAID-5 Volume איטיות יותר מאשר ב-Mirrored Volume. אולם, RAID-5 Volumes מספקים ביצועי קריאה טובים יותר מאשר Mirrored Volumes, במיוחד עם מספר בקרים, כיון שהנתונים מפוצלים בין מספר כוננים. עם זאת, כאשר דיסק כושל, ביצועי הקריאה ב-RAID-5 Volume מואטים בעת ש-Windows 2000 Server משחזרת את הנתונים שהיו בדיסק שכשל, על ידי שימוש במידע הזוגיות.

RAID-5 Volumes נהנים מיתרון מחירים ביחס ל-Mirrored Volumes כיון שיש אופטימיזציה לניצולת הדיסק. ככל שיש יותר דיסקים ב-RAID-5 Volume, כך קטנה עלות פס הנתונים היתיר. בטבלה הבאה מוצג, כיצד כמות המקום הדרושה לפס הנתונים קטנה עם הוספת דיסקים נוספים של 2GB ל-RAID-Volume :

מספר הדיסקים	מקום בשימוש בדיסק	מקום פנוי בדיסק	יתירות
3	6GB	4GB	33 אחוזים
4	8GB	6GB	25 אחוזים
5	10GB	8GB	20 אחוזים

קיימות מספר מגבלות ש-RAID-5 Volumes מיישמים בתוכנה. ראשית, RAID-5 Volumes מכילים לפחות שלושה כוננים ועד למספר מירבי של 32 כוננים. שנית, RAID-5 Volume ברמת התוכנה אינו יכול להכיל את מחיצת האתחול (Boot Partition) או את מחיצת המערכת (System Partition).

מערכת ההפעלה Windows 2000 אינה מודעת ליישומי RAID ברמת חומרה. לכן, המגבלות החלות על RAID ברמת התוכנה אינן חלות על תצורות RAID ברמת החומרה.

Mirrored Volumes versus RAID-5 Volumes

Mirrored Volumes ו-RAID-5 Volumes מספקים רמות שונות של fault tolerance. החלטה לגבי האפשרות הרצויה ליישום תלויה ברמת ההגנה הדרושה ובעלות החומרה. ההבדלים העיקריים בין RAID-1 Mirrored Volumes לבין RIAD-5 Volumes הם ביצועים ועלות.

הטבלה הבאה מתארת חלק מההבדלים בין RIAD-1 ברמת התוכנה ל- RAID-5.

RAID-1 **Mirrored Volumes**	**RAID-5** **Strip volumes with parity**
תומך ב-FAT ו-NTFS	תומך ב-FAT ו-NTFS
יכול להגן על מחיצת אתחול או מערכת	אינו יכול להגן על מחיצת אתחול או מערכת
דרושים שני דיסקים קשיחים	דרושים לפחות שלושה דיסקים קשיחים ומאפשר עד 32 דיסקים קשיחים
עלות גבוהה יותר לכל MB	עלות נמוכה יותר לכל MB
50 אחוזי ניצולת לשיקוף	מקסימום 33 אחוזי ניצולת למידע זוגיות
ביצועי כתיבה טובים	ביצועי כתיבה בינוניים
ביצועי קריאה טובים	ביצועי קריאה מעולים
משתמש בפחות זיכרון מערכת	משתמש ביותר זיכרון מערכת

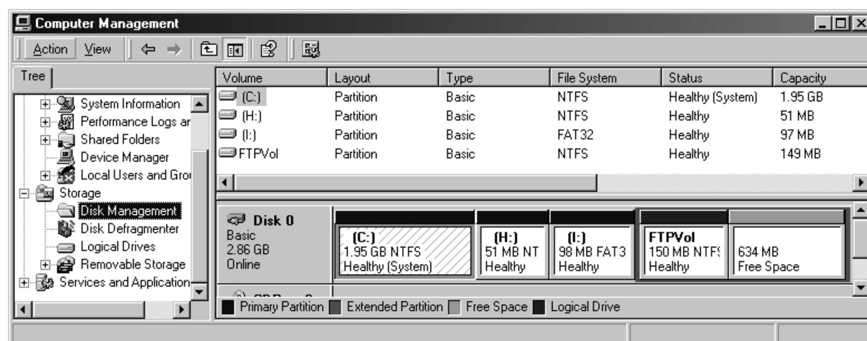
באופן כללי, Mirrored Volumes מציעים ביצועי קריאה וכתיבה המשתווים לאלה של דיסקים בודדים. RAID-5 Volumes מציעים ביצועי קריאה טובים יותר מאשר Mirrored Volumes, במיוחד עם מספר בקרים (Controllers), כיון שהנתונים מפוצלים בין מספר כוננים. עם זאת, הצורך לחשב מידע זוגיות דורש יותר זיכרון מערכת, דבר העלול להאט את הביצועים בזמן כתיבה.

Mirroring משתמש ב- 50 אחוזים משטח הדיסק הזמין בלבד, לכן שיטה זו יקרה יותר בעלות לכל MB ביחס לדיסקים ללא Mirroring. RAID-5 משתמש ב- 33 אחוזים מהמקום הפנוי בדיסק למידע זוגיות כאשר משתמשים במספר המינימלי של דיסקים קשיחים (שלושה). עם RAID-5, ניצולת הדיסק משתפרת ככל שמגדילים את מספר הדיסקים הקשיחים.

יישום מערכות RAID

תכונות Windows 2000 Server ל-Fault tolerance ברמת התוכנה זמינות רק עם דיסקים דינמיים של Windows 2000. ב- Windows 2000 Server, יוצרים Mirrored Volumes ו-RAID-5 Volumes ברמת התוכנה, על ידי שימוש באשף Create Volume בתוסף התוכנה Computer Management.

ליצירת Volume באמצעות אשף Create Volume, יש לגשת לתיקיה Disk Management בתוסף התוכנה Computer Management. כאשר בוחרים בתיקיה Disk Management, חלונית הפרטים של חלון Computer Management תציג טקסט של הדיסקים הפיסיים במחשב, ותצוגה גרפית (תרשים 12.13).



תרשים 12.13 התיקיה Disk Management בתוסף התוכנה Computer Management.

בחלונית הפרטים, בחר אזור בשטח שאינו מוקצה, ומתפריט Action הצבע על All Tasks, ולחץ על Create Volume. עקוב אחר השלבים המפורטים באשף Create Volume ליצירת volume.

הערה Windows 2000 Advanced Server ו- Windows 2000 Data Center תומכות באשכולות שרתים, למתן רמה גבוהה עוד יותר של Fault tolerance. אשכולות הם מעבר להיקף החומר הנלמד בספר זה.

סיכום שיעור

ניתן להגיע לרמה מסוימת של הגנה על ידי הגדרת UPS ועל ידי יישום Fault tolerance על דיסק. UPS מספק מתח במקרה של הפסקת חשמל מקומית. באופן כללי, UPS צריך לספק מתח למשך זמן מספיק לאזהרת משתמשים המחוברים לשרת ולביצוע כיבוי מסודר. ניתן להגדיר את שירות UPS בכרטיסיה UPS שבתיבת הדו-שיח Power Options Properties. לאחר הגדרת שירות UPS עבור המחשב, יש לבדוק את ההגדרות ולוודא שהמחשב מוגן מפני הפסקות חשמל. בנוסף להגנת מתח בעזרת UPS, RAID בעל Fault tolerance מספק רמה נוספת של הגנה על נתונים. ניתן להשתמש בתצורות Fault tolerance של RAID ליישום Fault tolerance על דיסק כפתרון תוכנה או כפתרון חומרה. Mirrored Volume ברמת התוכנה משתמש ב-Fault tolerance driver (Ftdisk.sys) של Windows 2000 Server לכתיבת אותם נתונים ל-volume בכל אחד משני דיסקים פיסיים בו-זמנית. Windows 2000 Server גם תומכת ב-Fault tolerance באמצעות Software-Level Striped Volumes With Parity - RAID 5. ב-RAID-5 Volumes, Windows 2000 משיגה Fault tolerance על ידי הוספת פס נתונים זוגי (Parity-Information Stripe) לכל מחיצת דיסק ב-Volume. באופן כללי, Mirrored Volumes מציעים ביצועי קריאה וכתיבה המשתווים לאלה של דיסקים בודדים. RAID-5 Volumes מציעים ביצועי קריאה טובים יותר ביחס ל-Mirrored Volumes. יישומי RAID נהנים משימוש במספר בקרים (שכפול דיסק) כיון שקלט/פלט של דיסק מפוצל בין מספר ערוצי נתונים להגברת ביצועים ו-fault tolerance. ניתן ליצור Mirrored Volumes ו-RAID-5 Volumes ברמת התוכנה באמצעות אשף Create Volume בתוסף התוכנה Computer Management, ועל דיסקים דינמיים בלבד.

שיעור 4: התאוששות מאסון

אמינות וזמינות מושפעות במידה מסוימת מיכולת המערכת להתאושש מאסון. התאוששות מאסון מאפשרת לשחזר מחשב, כך שניתן להיכנס ולגשת למשאבי המערכת לאחר התרחשות אסון. שיעור זה מספק מידע אודות תיקון התקנת Windows 2000, שחזור נתונים, ושחזור RAID-5 Volume או Mirrored Volume.

הערה למידע נוסף אודות אמינות וזמינות Windows 2000, עיין בתקליטור המצורף לספר זה (\chapt12\articles\Win2000Reliability.doc).

לאחר שיעור זה, תוכל:

- להשתמש ב-Safe Mode, ב-Recovery Console, ובדיסק תיקון החירום (Emergency Repair Disk) לתיקון התקנה של Windows 2000.
- לשחזר נתונים מגיבוי.
- לשחזר RAID-5 volume או RAID-1 volume.

זמן לימוד משוער: 60 דקות

תיקון התקנת Windows 2000

Windows 2000 כוללת מספר תכונות המאפשרות לתקן מערכת שאינה מאתחלת או אינה טוענת את Windows 2000. תכונות אלו שימושיות, אם חלק מקבצי המערכת נפגמו או שנמחקו בטעות, או אם הותקנה תוכנה, או שהותקנו מנהלי התקנים המונעים מהמערכת לפעול כראוי. Windows 2000 כוללת שלוש שיטות המאפשרות לתקן מערכת: מצב בטוח (Safe Mode), חלון התאוששות (Recovery Console), ודיסק תיקון חירום - ERD (**E**mergency **R**epair **D**isk).

הערה ניתן גם להתקין מחדש את Windows 2000 על פני מערכת Windows 2000 שנפגעה, או להתקין את Windows 2000 לתיקיה נפרדת. פעולות אלו עלולות לצרוך זמן רב, אולם הן שימושיות, אם הליך תיקון החירום אינו פותר את הבעיה. אם מתקינים מחדש את Windows 2000, ייתכן שיאבדו שינויים שבוצעו במערכת, כמו למשל שדרוגי חבילות שירות.

Safe Mode

מצב בטוח (Safe Mode) מאפשר להתחיל את המערכת עם מערכת מינימלית של מנהלי התקנים ושירותים. לדוגמה, אם מנהלי התקנים חדשים או תוכנה חדשה שהותקנו לאחרונה מונעים מהמחשב לאתחל, ייתכן שניתן יהיה לאתחל אותו במצב בטוח, ואז להסיר את התוכנה או ההתקנים מהמערכת. מצב בטוח אינו פועל בכל הנסיבות, במיוחד אם קבצי המערכת פגומים או חסרים, או אם הדיסק הקשיח נפגם או כשל.

במצב בטוח, Windows 2000 משתמשת בהגדרות ברירת מחדל (צג VGA, מנהל התקן עכבר של Microsoft, ומנהלי ההתקנים המינימליים הדרושים להפעלת Windows). אם תופעה מסוימת אינה חוזרת על עצמה כאשר מפעילים במצב בטוח, ניתן לשלול את הגדרות ברירת המחדל ואת מנהלי ההתקנים המינימליים, כגורמים אפשריים לבעיה.

ניתן לבחור אחת מהאפשרויות הבאות, כאשר מאתחלים במצב בטוח:

- **Safe Mode** – מאתחל את Windows 2000 ומשתמש רק בקבצים ומנהלי התקנים בסיסיים (עכבר, מלבד עכבר טורי; צג; מקלדת; אמצעי אחסון; תצוגת VGA בסיסית; שירותי מערכת ברירת מחדל; ללא חיבורים לרשת). אם המחשב אינו מאתחל בהצלחה במצב בטוח, ייתכן שתצטרך להשתמש ב-ERD לתיקון המערכת.
- **Safe Mode With Networking** – מאתחל את Windows 2000 עם קבצים ומנהלי התקנים בסיסיים בלבד, בתוספת חיבורי רשת.
- **Safe Mode With Command Prompt** – מאתחל את Windows 2000 עם קבצים ומנהלי התקנים בסיסיים בלבד. לאחר הכניסה, מוצג מנחה שורת הפקודה (Command Prompt) במקום שולחן העבודה של Windows.
- **Enable Boot Logging** – מאתחל את Windows 2000, תוך רישום כל מנהלי ההתקנים והשירותים המותקנים אשר נטענו (או שלא נטענו) על ידי המערכת לקובץ יומן. קובץ זה נקרא ntbtlog.txt וממוקם בספריה %systemroot%. מצבי האתחול Safe Mode, Safe Mode With Networking, ו- Safe Mode With Command Prompt מוסיפים ל**יומן** האתחול (Boot Log) רשימה של כל מנהלי ההתקנים והשירותים הנטענים. יומן האתחול שימושי בקביעת הגורם המדויק לבעיות אתחול המערכת.
- **Enable VGA Mode** – מאתחל את Windows 2000 עם מנהל התקן VGA הבסיסי. מצב זה שימושי, כאשר הותקן מנהל התקן חדש עבור מתאם התצוגה הגורם ל- Windows 2000 שלא לאתחל כנדרש. מנהל התקן תצוגה הבסיסי משמש גם כאשר מאתחלים את Windows 2000 במצב בטוח (Safe Mode, Safe Mode With Networking, או Safe Mode With Command Prompt).

* **Last Known Good Configuration** – מאתחל את Windows 2000 עם המידע האחרון השמור ברישום המערכת (Registry) מאז אתחול אחרון מוצלח של Windows. השתמש באפשרות זו רק במקרים של הגדרות שגויות. Last Known Good Configuration (תצורה מוצלחת ידועה אחרונה) אינו פותר בעיות שנגרמו על ידי קבצים או מנהלי התקנים פגומים, חסרים או לא-מתאימים. בנוסף, שינויים כלשהם, שבוצעו מאז האתחול המוצלח האחרון - יאבדו.
* **Directory Service Restore Mode** – משמש לשחזור הספריה SYSVOL ושירותי Active Directory ב-DC. אפשרות זו זמינה ב-DCs בלבד.
* **Debugging Mode** – מאתחל את Windows 2000, תוך שליחת מידע איתור תקלות דרך כבל טורי למחשב אחר. זהו מצב חשוב עבור אנשי פיתוח תוכנה.

אם משתמשים או שנעשה בעבר שימוש בשירותי התקנה מרחוק (RIS - **R**emote **I**nstall **S**ervices) להתקנת Windows 2000 על המחשב, ייתכן שיוצגו אפשרויות נוספות הקשורות לשחזור או התאוששות המערכת דרך שירותי התקנה מרחוק.

לאתחול Windows 2000 במצב בטוח, הפעל מחדש את המחשב. הקש F8 כאשר מוצגת ההודעה Please Select The Operating System To Start. השתמש במקשי החיצים להארת אפשרות המצב הבטוח הרצויה, ואז הקש Enter.

מצב בטוח מסייע באבחון בעיות. אם תופעה מסוימת אינה חוזרת כאשר מפעילים את המחשב במצב בטוח, ניתן לשלול את הגדרות ברירת המחדל ואת מנהלי ההתקנים המינימליים כגורמים אפשריים לבעיה. אם התקן חדש או מנהל התקן (Driver) שהוחלף הם הגורמים לבעיה, ניתן להשתמש במצב הבטוח להסרת ההתקן או לביטול השינוי.

Recovery Console

ה-Recovery Console, למרות שהוא נראה כמו שורת הפקודה (command prompt) של Windows 2000, הוא חלון בקרה נפרד המאפשר למנהל המערכת לגשת לדיסק הקשיח של מחשב המפעיל Windows 2000, ללא תלות במערכת הקבצים (NTFS או FAT) שבשימוש, לצורך איתור תקלות ותחזוקת מערכת בסיסית. הפעלת Windows 2000 אינה תנאי מוקדם לשימוש ב-Recovery Console. אפשרות זו יכולה לסייע בהתאוששות, כאשר מחשב המבוסס על Windows 2000 אינו מאתחל בהצלחה, או אינו מאתחל כלל.

חלון ההתאוששות מאפשר גישה מוגבלת ל-volumes של NTFS, FAT16 ו-FAT32, בלי להפעיל את הממשק הגרפי. חלון ההתאוששות מאפשר למנהלים ולטכנאים של שירותי תמיכת מוצרים של Microsoft להפעיל ולהפסיק שירותים (Enable/Disable services), ולתקן את המערכת באופן פרטני ביותר. ניתן להשתמש באפשרות זו לתיקון רשומת האתחול העיקרית (MBR) וסקטור האתחול (Boot Sector) ולפרמוט Volumes. חלון התאוששות מונע גישה בלתי מאושרת ל-Volumes, על ידי דרישה מהמשתמש להזין סיסמת Administrator.

הפעלת Recovery Console

להפעלת חלון ההתאוששות (Recovery Console), הפעל את המחשב מתקליטור ההתקנה של Windows 2000 או מהדיסקטים של Windows 2000 Setup. אם אין ברשותך דיסקטים להתקנת מערכת ההפעלה, והמחשב אינו יכול לאתחל מתקליטור ההתקנה של Windows 2000, השתמש במחשב אחר ובתוכנית השירות Makeboot.exe או Makebt32.exe ליצירת ערכת הדיסקטים של התקנת Windows 2000.

אם חלון ההתאוששות הותקן על הדיסק הקשיח המקומי, ניתן לגשת אליו גם מתפריט האתחול של Windows 2000. אולם, אם רשומת האתחול העיקרית או סקטור האתחול של system volume נפגמו, יש לאתחל את המחשב באמצעות דיסקטים של Windows 2000 Setup, או באמצעות תקליטור ההתקנה של Windows 2000, כדי לגשת לחלון ההתאוששות.

להוספת חלון ההתאוששות להתקנות קיימות של Windows 2000, בתפריט Start, לחץ על Run, והקלד **<cdrom>:\I386\Winnt32.exe/cmdcons**, כאשר <cdrom> היא אות הכונן המייצגת את כונן התקליטורים במערכת.

התקנה זו של חלון ההתאוששות דורשת כ- 7MB של מקום פנוי בדיסק במחיצת המערכת.

חשוב **לא ניתן להתקין מראש את חלון ההתאוששות על מחשב המכיל Mirrored Volume. יש לשבור תחילה את ה- Mirroring, ואז להתקין את חלון ההתאוששות. לאחר התקנת חלון ההתאוששות, ניתן ליצור מחדש את ה-Mirrored Volume.**

אם חלון ההתאוששות אינו מותקן, הפעל את Windows 2000 Setup. לחץ על Enter במסך Setup Notification. הקש על R לתיקון התקנה של Windows 2000, ואז הקש על C לשימוש בחלון ההתאוששות (Recovery Console).

התקנות והגדרות תצורה מסוימות עלולות להשפיע על אופן השימוש בחלון ההתאוששות:

- אם יש יותר מהתקנה אחת של Windows 2000 או Windows NT 4.0 או מוקדם יותר, הן מוצגות בתפריט Recovery Console Startup.
- Mirrored Volumes מוצגים פעמיים בתפריט Recovery Console Startup, אולם לכל ערך יש אותה אות כונן, לכן הם למעשה אותו כונן.
- שינויים המבוצעים בעזרת חלון ההתאוששות ל-Mirrored Volumes ישוכפלו.

כדי לגשת לדיסק באמצעות חלון ההתאוששות, הקש על מקש המספר המייצג את התקנת Windows 2000 שאותה רוצים לתקן, ואז הקש Enter. חלון ההתאוששות מבקש את סיסמת האדמיניסטרטור. אם מקישים Enter מבלי להזין סיסמה, חלון ההתאוששות יוצא ומאתחל את המחשב מחדש.

הערה כדי להשתמש בחלון ההתאוששות, יש לדעת את הסיסמה של חשבון Administrator המקומי. אם לא ידועה הסיסמה הנכונה, חלון ההתאוששות אינו מאפשר גישה למחשב. אם מוזנת סיסמה שגויה שלוש פעמים, חלון ההתאוששות יוצא ומאתחל את המחשב מחדש. ניתן להשתמש בתוסף התוכנה Group Policy או בתוסף התוכנה Security Configuration And Analysis, כדי לאפשר כניסה אוטומטית של מנהלים. הגדרה זו נכללת בצומת Security Options, ושם הערך הוא Recovery Console: Allow Automatic Administrative Logon.

לאחר אימות הסיסמה, מתקבלת גישה מלאה לחלון ההתאוששות, וגישה מוגבלת לדיסק הקשיח. ניתן לגשת למחיצות ולתיקיות הבאות במחשב:

- %systemroot% ותיקיות משנה של התקנת Windows 2000 אליה נכנסת.
- שורש של כל המחיצות, כולל %systemdrive%, התקליטור, וכונן הדיסקטים עם הגבלות מסוימות (הגבלות כונן דיסקטים מוצגות בהמשך שיעור זה).

הערה כאשר הפקודה set מופעלת, ניתן להעתיק קבצים אל אמצעים הניתנים להסרה, לבטל את - File Copy Prompt, להשתמש בתווי הכללה (כוכבית וסימן שאלה) עם הפקודה Copy, ולגשת לכל הנתיבים במערכת. הפקודה Set היא פקודה אופציונלית של חלון ההתאוששות, אותה ניתן להוסיף באמצעות תוסף התוכנה Group Policy או תוסף התוכנה Security Configuration And Analysis.

חלון ההתאוששות מונע גישה לתיקיות אחרות, כגון Program Files או Documents And Settings, בנוסף לתיקיות המכילות התקנות אחרות של Windows 2000. עם זאת, ניתן להשתמש בפקודות logon לגישה אל התקנה חלופית. לחילופין, ניתן לגשת לתיקיות התקנה אחרות על ידי הפעלה מחדש של חלון ההתאוששות, בחירת המספר המייצג את ההתקנה הרצויה, ואז הזנת סיסמת המנהל עבור התקנה זו.

לא ניתן להעתיק קובץ מהדיסק הקשיח המקומי לדיסקט, אולם ניתן להעתיק קובץ מדיסקט או תקליטור אל דיסק קשיח כלשהו, ומדיסק קשיח לדיסק קשיח אחר. אולם, כאשר הפקודה Set מופעלת, ניתן להעתיק קבצים אל דיסקט. חלון ההתאוששות מציג הודעת שגיאה Access Is Denied, כאשר הוא מזהה פקודות לא חוקיות.

חשוב הפקודה Set משתמשת במשתני סביבה של חלון ההתאוששות, כדי לאפשר גישת כתיבה לדיסק עבור דיסקטים בנוסף להפעלת אפשרויות אחרות. כדי לאפשר למשתמש לשנות את ברירת המחדל של משתני הסביבה המוגבלים של חלון ההתאוששות, יש לבצע הגדרת מדיניות.

חלון ההתאוששות אוגר בחוצץ (Buffer) פקודות שהוזנו קודם לכן, וגורם להן להיות זמינות למשתמש בעזרת מקשי החיצים מעלה ומטה. לעריכת פקודה שהוזנה בעבר, השתמש ב-Backspace להזזת הסמן אל נקודת העריכה, והקלד מחדש את יתר הפקודה. בנקודה כלשהי, ניתן לצאת מחלון ההתאוששות ולאתחל מחדש את המחשב על ידי הקלדת **exit** בשורת הפקודה.

שים לב שחלון ההתאוששות עשוי למפות disk volumes באותיות כונן שונות מאלו המוקצות ב-Windows 2000. אם מתעוררים קשיים בהעתקת קבצים ממיקום אחד לאחר, השתמש בפקודה Map מתוך חלון ההתאוששות, כדי לוודא שמיפויי הכוננים נכונים, הן עבור המקור והן עבור היעד.

טיפ ניתן להשתמש בפקודה Help להצגת רשימה של הפקודות הנתמכות על ידי חלון ההתאוששות. בנוסף, המתג /? פועל עם כל פקודת חלון ההתאוששות, להצגת מסך עזרה עם תיאור של הפקודה, התחביר שלה, הגדרה של הפרמטרים ומידע שימושי נוסף.

דיסק תיקון חירום

אם המערכת אינה מתחילה, ושימוש במצב בטוח או בחלון ההתאוששות לא הועילו, ניתן לנסות להשתמש ב**דיסק תיקון חירום** (**E**mergency **R**epair **D**isk - ERD). תוכנית Backup כוללת אשף המסייע ליצור ERD. אם מתרחשת תקלה במערכת, ראשית הפעל את המערכת באמצעות תקליטור ההתקנה של Windows 2000 או דיסקטים של Windows 2000 Setup, שאותם ניתן ליצור על ידי הפעלת Makeboot.exe או Makebt32.exe מהתיקיה Bootdisk שבתקליטור ההתקנה של Windows 2000. במצב Text, הקלד **R** כדי להיכנס ל-Recovery Options והקלד **R** שוב לכניסה ל- Emergency Repair. אז, השתמש ב-ERD לשחזור קבצי ליבת המערכת (Kernel). שים לב שלא ניתן לתקן את כל בעיות הדיסק באמצעות ERD.

הקפד ליצור ERD כאשר המחשב מתפקד כהלכה, כדי שתהיה מוכן במקרה שיהיה צורך לתקן קבצי מערכת. ניתן להשתמש ב-ERD לתיקון בעיות שאולי מונעות את הפעלת המחשב. הדבר כולל בעיות ברישום, קבצי מערכת, סקטור מחיצת האתחול, וסביבת האתחול. עם זאת, ERD אינו מגבה נתונים או תוכניות ואינו מהווה תחליף לגיבויי מערכת סדירים.

ERD של Windows 2000, שלא כמו ERD המשמש עם Windows NT, אינו מכיל עותק של קבצי הרישום. קבצי גיבוי של הרישום נמצאים בתיקיה %systemroot%\Repair כמו ב-Windows NT, אולם קבצים אלה נוצרו בזמן ההתקנה המקורית של Windows 2000. במקרה של בעיה, ניתן להשתמש בהם להחזרת המחשב למצב בר-שימוש.

אזהרה במידה והשתמשת בקבצי רישום מתיקיית Repair לתיקון, **יימחקו** כל החשבונות (קבוצות, משתמשים, מחשבים) שיצרת. **יישארו** רק החשבונות המובנים (Build-in) **שנוצרו** בעת ההתקנה, כגון Administrator **ו-**Guest.

כאשר מגבים נתוני מצב מערכת (System State Data), עותק של קבצי הרישום מוצב בתיקיה systemroot%\Repair\Regback%. אם קבצי הרישום נפגמים או נמחקים בטעות, השתמש בקבצים שבתיקיה זו לתיקון הרישום, בלי לבצע שחזור מלא של נתוני מצב המערכת. שיטה זו מומלצת למשתמשים מתקדמים בלבד וניתנת לביצוע גם באמצעות פקודות חלון ההתאוששות.

ERD - Emergency Repair Disk

בעת יצירת ERD, הקבצים המתוארים בטבלה מועתקים מ- systemroot%\Repair% לדיסקט.

שם קובץ	תוכן
Autoexec.nt	עותק של systemroot%\System32\Autoexec.nt% המשמש לאתחול סביבת MS-DOS.
Config.nt	עותק של systemroot%\System32\Config.nt% המשמש לאתחול סביבת MS-DOS.
Setup.log	יומן המכיל רשימה של כל קבצי המערכת שהותקנו ושל מידע בדיקת יתירות מעגלית - CRC (**C**yclic **R**edundancy **C**heck) לשימוש בהליך תיקון החירום. לקובץ זה יש מאפייני קריאה בלבד, מערכת ומוסתר, והוא אינו נראה, אלא אם ב- My Computer הוגדרה האפשרות להצגת כל הקבצים, או שנעשה שימוש בפקודות שורת הפקודה dir, dir /a, dir /as או dir /ah.

צור את ERD לאחר התקנת Windows 2000. צור מחדש את ERD לאחר כל התקנת חבילת שירות, עדכון מערכת, או עדכון מנהל התקן. הקפד להכין עותק עדכני של ERD ולאחסן אותו במקום מוגן, אולי אף במקום אחר.

הליך תיקון חירום

אם הכנת ERD תוכל להשתמש בו כסיוע לתיקון קבצי מערכת לאחר אתחול המחשב באמצעות תקליטור ההתקנה של Windows 2000 או באמצעות דיסקטי Windows 2000 Setup. אולם, תקליטור ההתקנה של Windows 2000 נדרש בכל מקרה להחלפת קבצים פגומים כלשהם.

ERD חייב לכלול מידע הגדרות תצורה עדכני. יש להקפיד שיהיה ERD עבור כל אחת מהתקנות Windows 2000 במחשב, ורק במקרים מסויימים ניתן להשתמש ב-ERD של מחשב אחר, כגון מצב בו יש לתקן את MBR ולא נעשה שימוש בתוכן דיסקט ERD.

כאשר תתחיל את הליך תיקון החירום, תתבקש לבחור אחת מבין האפשרויות הבאות:

- **Manual Repair** – לבחירה מרשימה של אפשרויות תיקון, הקש **M**. מומלץ שרק משתמשים מתקדמים או מנהלים יבחרו באפשרות זו. על ידי שימוש באפשרות זו ניתן לתקן קבצי מערכת, בעיות בסקטור האתחול ובעיות בסביבת האתחול.

- **Fast Repair** – לביצוע כל אפשרויות התיקון, הקש **F**. זוהי האפשרות הקלה יותר לשימוש, והיא אינה דורשת נתונים מהמשתמש. אם בוחרים באפשרות זו, הליך התאוששות חירום מנסה לתקן בעיות הקשורות לקבצי מערכת, סקטור האתחול בדיסק המערכת, וסביבת האתחול (אם מותקנות במחשב מספר מערכות הפעלה). אפשרות זו גם בודקת ומתקנת את קבצי הרישום על ידי טעינה והסרת כל מפתח רישום. אם מפתח אינו נבדק בהצלחה, הוא מועתק אוטומטית מתיקיית התיקון לתיקיה %systemroot%\System32\Config.

אם בוחרים Manual Repair, קבצי הרישום אינם נבדקים. אם בוחרים Fast Repair, והתיקיה %systemroot%\Repair זמינה, קבצי הרישום נבדקים. אם התיקיה %systemroot%\Repair אינה זמינה (למשל כתוצאה מפגיעה במערכת הקבצים), קבצי הרישום לא נבדקים.

תיקון ידני מאפשר לבחור מבין שלוש האפשרויות הבאות:

- **Inspect Startup Environment**. אפשרות זו בודקת שקבצי Windows 2000 במחיצת המערכת נכונים. אם אחד מהקבצים הדרושים להפעלת Windows 2000 חסר או פגום, Repair מחליף אותו מתקליטור ההתקנה של Windows 2000. קבצים אלה כוללים את Ntldr ואת Ntdetect.com. אם Boot.ini חסר, הוא נוצר מחדש.

- **Verify Windows 2000 System Files**. אפשרות זו משתמשת בסכום ביקורת (Checksum) לוודא שכל קובץ מותקן הוא טוב ותואם לקובץ שהותקן מתקליטור ההתקנה של Windows 2000. אם הליך ההתאוששות קובע שקובץ בדיסק אינו תואם את מה שהותקן, הוא מציג הודעה המזהה את הקובץ, ושואלת אם ברצונך להחליפו. הליך תיקון החירום גם מוודא שקבצי אתחול, כגון Ntldr ו-Ntoskrnl.exe, נמצאים ותקינים.

- **Inspect Boot Sector** (בדיקת סקטור האתחול). אפשרות זו מוודאת שסקטור האתחול במחיצת המערכת עדיין מתייחס ל-Ntldr. הליך תיקון החירום יכול רק להחליף את סקטור האתחול עבור מחיצת המערכת בדיסק הקשיח הראשון. הליך תיקון החירום יכול גם לתקן את סקטור האתחול עבור מחיצת המערכת בדיסק Startup.

הערה אם סקטור האתחול נדבק בווירוס, אתחל את המחשב באמצעות דיסקט אתחול של תוכנית אנטי-וירוס. הורה לתוכנית האנטי-וירוס לבדוק ולרפא את סקטור האתחול. תוכנית אנטי-וירוס לבדיקת סקטור האתחול נכללת בתקליטור ההתקנה של Windows 2000 Server בתיקיה \3RDPARTY\CA_ANTIV.

אם הליך תיקון החירום אינו מתקן את המערכת

אם ביצעת את הליך תיקון החירום, והמחשב עדיין אינו פועל כנדרש, ניתן לבצע שידרוג מקומי על גבי ההתקנה הקיימת. זוהי הברירה האחרונה לפני התקנה מחדש של מערכת ההפעלה. עם זאת, שים לב שהזמן הנדרש לביצוע שידרוג דומה לזמן הנדרש להתקנה מחדש של מערכת ההפעלה.

הערה אם מבצעים שידרוג מקומי של ההתקנה הקיימת של Windows 2000, **ייתכן שיאבדו** מספר הגדרות מותאמות אישית של קבצי המערכת.

שחזור נתונים

היכולת לשחזר נתונים פגומים או אבודים היא קריטית לכל חברה, והיא המטרה של כל פעולות הגיבוי. כדי להבטיח שניתן לשחזר בהצלחה נתונים, כדאי לפעול לפי הנחיות מסוימות, כגון שמירת תיעוד יסודי של כל פעולות הגיבוי. בנוסף, יש לבחור את מערכות הגיבוי, קבצים, ותיקיות לשחזור. ניתן גם לציין הגדרות נוספות על סמך דרישות השחזור. Windows Backup מספק אשף Restore המסייע בשחזור נתונים, או לחילופין, ניתן לשחזר נתונים בלי להשתמש באשף.

הכנה לשחזור נתונים

כאשר נתונים קריטיים אובדים, יש לשחזר את הנתונים במהירות. השתמש בהנחיות הבאות להכנה לשחזור נתונים:

- ❖ בסס את אסטרטגיית השחזור על סוג הגיבוי ששימש לגיבוי הנתונים. אם הזמן קריטי בעת שחזור הנתונים, אסטרטגיית השחזור צריכה להבטיח שסוגי הגיבוי שנבחרו לגיבוי מזרזים את הליך השחזור. לדוגמה, השתמש בגיבויים רגילים (Normal) ומשתנים (Differential), כדי שיהיה צורך לשחזר רק את הגיבוי הרגיל האחרון ואת הגיבוי המשתנה האחרון.
- ❖ בצע שחזור ניסיון באופן סדיר כדי לוודא ש- Windows Backup מגבה את הקבצים כנדרש. שחזור ניסיון יכול לחשוף בעיות חומרה שאינן נראות באימות גיבוי קבצים. שחזר את הנתונים למקום חלופי, ואז השווה בין הנתונים המשוחזרים לבין הנתונים בדיסק הקשיח המקורי.

- שמור תיעוד של כל פעולת גיבוי. צור והדפס יומן גיבוי מפורט עבור כל פעולת גיבוי. יומן גיבוי מפורט כולל רישום כל הקבצים והתיקיות שגובו. על ידי שימוש ביומן הגיבוי, ניתן לאתר בקלות איזה חלק של מדיה מכיל את הקבצים הדרושים לשחזור בלי צורך לטעון את הקטלוגים. **קטלוג** (Catalog) הוא אינדקס של הקבצים והתיקיות מפעולת גיבוי ש- Windows 2000 יוצרת אוטומטית ומאחסנת עם פעולת הגיבוי על המחשב המפעיל את Windows Backup.

- שמור רישום של פעולות גיבוי מרובות בתבנית לוח שנה המציג את הימים בהם מבוצעות פעולות הגיבוי. עבור כל פעולה, ציין את סוג הגיבוי וזהה את אמצעי האחסון שבשימוש, כגון מספר הטייפ או שם הדיסק הניתן להסרה. אז, אם יש צורך לשחזר נתונים, ניתן יהיה לסקור בקלות פעולות גיבוי של מספר שבועות לבחירת הסוג הרצוי לשימוש.

בחירת מערכות גיבוי, קבצים ותיקיות לשחזור

השלב הראשון בשחזור נתונים הוא בחירת הנתונים לשחזור. ניתן לבחור קבצים ותיקיות בודדים, פעולת גיבוי שלמה, או מערכת גיבוי. **ערכת גיבוי** (Backup Set) היא אוסף קבצים או תיקיות מ-volume אחד אשר מגובים בפעולת גיבוי. אם מגבים שני volumes בדיסק קשיח בפעולת גיבוי אחת, לפעולת גיבוי זו יש שתי ערכות גיבוי. ניתן לבחור את הנתונים לשחזור מהקטלוג.

לשחזור נתונים השתמש באשף Restore, שאליו ניתן לגשת דרך Windows Backup. לאחר הפעלת האשף, ההגדרות הראשוניות להליך השחזור מוצגות במסך Completing The Restore Wizard. בשלב זה, ניתן לבצע אחת מהפעולות הבאות:

- סיום הליך השחזור על ידי לחיצה על הלחצן Finish. אם בוחרים לסיים את פעולת השחזור, אשף Restore מבקש אימות למקור מדיה השחזור, ואז מבצע את השחזור. בעת הליך השחזור, מציג אשף Restore מידע אודות מצב השחזור.

- ציון אפשרויות שחזור מתקדמות על ידי לחיצה על הלחצן Advanced.

ציון הגדרות שחזור מתקדמות

ההגדרות המתקדמות באשף Restore משתנות, בהתאם לסוגים של אמצעי הגיבוי שממנו מבוצע השחזור. לאחר סיום אשף Restore, Windows Backup מבצע את הפעולות הבאות:

- ❖ מבקש אימות של בחירת המדיה שתשמש לשחזור נתונים. לאחר האימות, מתחיל Windows Backup את הליך השחזור.
- ❖ מציג מידע אודות מצב הליך השחזור. כמו בהליך הגיבוי, ניתן לבחור להציג את דוח השחזור (Restore Log). הדוח מכיל מידע אודות השחזור, כגון מספר הקבצים ששוחזרו ומשך הליך השחזור.

הטבלה הבאה מתארת את אפשרויות השחזור המתקדמות.

אפשרות	תיאור
Restore Files To	מיקום היעד עבור הנתונים המשוחזרים. ניתן לבחור מבין האפשרויות הבאות: • **Original Location** - משחזר נתונים למיקומם המקורי. • **Alternate Location** - משחזר נתונים למיקום חילופי. תתבקש לציין את המסלול (path) לשחזור הנתונים. • **Single Folder** - מאחד את הקבצים ממבנה עץ לתיקיה יחידה. לדוגמה, השתמש באפשרות זו אם רצונך בעותקים של קבצים מסוימים אולם אינך רוצה לשחזר את המבנה ההירכי של הקבצים. אם בוחרים במיקום חלופי או בתיקיה יחידה, יש לספק את הנתיב הרצוי.
When Restoring A File That Is Already On My Computer	האפשרויות האם להחליף קבצים קיימים או לא. ניתן לבחור מבין האפשרויות הבאות: • **Do Not Replace The File On My Disk (Recommended)** אפשרות זו מונעת כתיבה בטעות על נתונים קיימים. אפשרות זו היא ברירת המחדל. • **Replace The File On My Disk Only If The File On Disk Is Older Than The Backup Copy** - מוודא שהעותק העדכני ביותר קיים במחשב. • **Always Replace The File On My Computer** - Windows Backup אינו מציג הודעה אם הוא נתקל בשם קובץ כפול בעת הליך השחזור.

אפשרות	תיאור
Advanced Restore Options	האפשרויות האם לשחזר קבצי אבטחה או קבצי מערכת מיוחדים או לא. ניתן לבחור מבין האפשרויות הבאות: • **Restore Security** - מחיל את ההרשאות המקוריות לקבצים המשוחזרים ל-NTFS volume. הגדרות אבטחה כוללות הרשאות גישה, רישומי ביקורת, ובעלות. אפשרות זו זמינה רק אם גיבוי הנתונים בוצע מ-NTFS volume והשחזור מבוצע ל-NTFS volume. • **Restore Removable Storage Database** - משחזר את מסד הנתונים האחראי לניהול התקנים הניתנים להסרה (**R**emovable **S**torage **M**anagement) ואת הגדרות מאגר המדיה. מסד הנתונים ממוקם ב- %systemroot%\system32\remotestorage. %systemroot%\system32\NTmsData. • **Restore Junction Points, And Restore File And Folder Data Under Junction Points To The Original Location** משחזר נקודות צומת לדיסק הקשיח בנוסף לנתונים אליהם מתייחסות נקודות הצומת. אם כוננים מותקנים פיסית, ורוצים לשחזר את הנתונים שכוננים אלה מצביעים אליהם, כדאי לסמן תיבת סימון זו. אם לא מסמנים אפשרות זו, נקודת הצומת תשוחזר, אולם ייתכן שהנתונים אליהם מתייחסת נקודת הצומת לא יהיו נגישים.

תרגיל 2: שחזור נתונים

בתרגיל זה, תמחק את התיקיה Inetpub ואז תפעיל שגרת שחזור לשחזורה. בצע תרגיל זה על Server01.

הליך 1: מחיקת נתונים קריטיים

בהליך זה, תמחק בכוונה את Boot.ini. בדרך כלל, מחיקת קבצים קריטיים היא טעות או תוצאה של כשל חומרה.

1. לחץ לחיצה כפולה על My Computer, ולחץ לחיצה כפולה על Local Disk (C:).

   יופיע החלון Local Disk (C:).
2. הגדל את החלון לגודל מירבי.
3. פתח את תפריט Tools, ולחץ על Folder Options. תופיע תיבת הדו-שיח Folder Options.
4. בחר בכרטיסיה View.

5. נקה את תיבת הסימון Hide Protected System Files (Recommended).

תופיע תיבה של הודעת אזהרה, שכעת יופיעו קבצים קריטיים מוסתרים וקבצי מערכת.

6. לחץ Yes. תופיע תיבת הדו-שיח Folder Options.

7. לחץ OK. יופיעו קבצים נוספים בחלון Local Disk (C:).

8. לחץ פעם אחת על boot.ini.

9. פתח את תפריט File, ולחץ Delete. תופיע תיבת הודעה Confirm File Delete ובה שאלה האם אתה בטוח שברצונך למחוק קובץ קריטי זה.

10. לחץ Yes.

הקובץ Boot.ini אינו קיים עוד. למרות שניתן לשחזר אותו מסל המחזור (Recycle Bin), נשתמש בתוכנית השחזור בהליך הבא, לשחזור הקובץ שגובה בתרגיל 1.

11. השאר את החלון Local Disk (C:) בגודל מלא; הוא ישמש אותך גם בהליך הבא.

הליך 2: שחזור נתונים קריטיים

בהליך זה תשחזר את Boot.ini ממערכת הגיבוי.

1. בחלון Local Disk (C:), לחץ לחיצה כפולה על Backup1.bkf.

תופיע תיבת הדו-שיח Backup - [Untitled].

2. לחץ על הלחצן Restore Wizard. יופיע מסך Welcome To The Restore Wizard.

3. לחץ Next. יופיע המסך What To Restore, ובו בקשה לבחור את אמצעי הגיבוי שממנו ברצונך לשחזר קבצים.

שים לב שהאמצעי היחיד שממנו ניתן לשחזר הוא קובץ, וקבצי הגיבוי רשומים בהתאם לתווית האמצעי המצוינת.

4. תחת התיבה What To Restore, הרחב את פעולת הגיבוי הראשונה שיצרת בתרגיל 1.

שים לב שכונן C יוצג כתיקיה הראשונה בקובץ הגיבוי. Windows Backup יוצר מערכת גיבוי שונה עבור כל volume מגובה. כל התיקיות והקבצים המגובים מ-volume בודד יופיעו תחת אות הכונן עבור volume זו.

5. הרחב את כונן C. תופיע תיבת הדו-שיח Backup File Name ובתיבת הטקסט Catalog Backup File רשום C:\Backup1.bkf.

אם יופיע C:\Backup2.bkf, שנה את השם ל- C:\Backup1.bkf.

6. לחץ OK.

7. כאשר תוחזר למסך What To Restore, לחץ על :C. בעמודה Name יופיע Boot.ini.

8. בעמודה Name, סמן את תיבת הסימון Boot.ini, ולחץ Next.

יופיע המסך Completing The Restore Wizard, ובו תתבקש להתחיל את פעולת השחזור, ולהשתמש בהגדרות ברירת המחדל לשחזור.

9. לחץ Advanced. יופיע המסך Where To Restore, ובו תתבקש להזין מיקום יעד לשחזור קבצים.

10. לחץ על תיבת הרשימה הנפתחת להצגת אפשרויות מיקום השחזור.

11. ודא שנבחר Original Location, ולחץ Next.

12. יופיע המסך How To Restore, ובו תתבקש לציין כיצד לעבד קבצים כפולים בעת ביצוע השחזור.

13. ודא שלחצן האפשרות Do Not Replace The File On My Disk (Recommended) נבחר, ולחץ Next.

14. יופיע המסך Advanced Restore Options, ובו תתבקש לבחור אפשרויות אבטחה עבור פעולת השחזור.

15. ודא שתיבת הסימון Restore Security מסומנת, נקה את תיבת הסימון Restore Junction Points, Not The Folders And File Data They Reference, ולחץ Next.

יופיע המסך Completing The Restore Wizard, ובו סיכום אפשרויות השחזור הנבחרות.

16. לחץ Finish להתחלת הליך השחזור. Windows Backup יציג את תיבת הדו-שיח Enter Backup File Name, ובה תתבקש לספק או לאמת את שם קובץ הגיבוי המכיל את התיקיות והקבצים המיועדים לשחזור.

17. ודא שמוזן C:\Backup1.bkf בתיבת הטקסט Restore From Backup File, ולחץ OK.

תופיע תיבת הדו-שיח Selection Information.

תופיע תיבת הדו-שיח Restore Progress, המציגה את מצב פעולת השחזור, סטטיסטיקה אודות כמות הנתונים המשוערת וכמות הנתונים בפועל המעובדים, הזמן שחלף, והערכה לזמן שנותר להליך השחזור.

18. כאשר תיבת הדו-שיח Restore Progress מציינת שהושלם השחזור, לחץ Report.

Notepad מופעל ומציג את הדוח. שים לב שהפרטים אודות פעולת השחזור מתוספים בסוף יומן הגיבוי. הדבר מספק מיקום מרכזי, ממנו ניתן להציג את כל מידע המצב עבור פעולת שחזור וגיבוי זו.

19. קרא את הדוח, וסגור את Notepad.

20. בתיבת הדו-שיח Restore Progress, לחץ Close.

תופיע תיבת הדו-שיח Backup - [Untitled] ובה הכרטיסיה Welcome פעילה.

21. סגור את תיבת הדו-שיח Backup - [Untitled]. יופיע החלון Local Disk (C:).

22. שים לב שהקובץ Boot.ini שוחזר.

23. סגור את החלון Local Disk (C:).

שחזור RAID-5 Volume או Mirrored Volume

סעיף זה מספק מידע אודות התאוששות מכשל ב-Mirroed Volume ותיקון RAID-5 Volume.

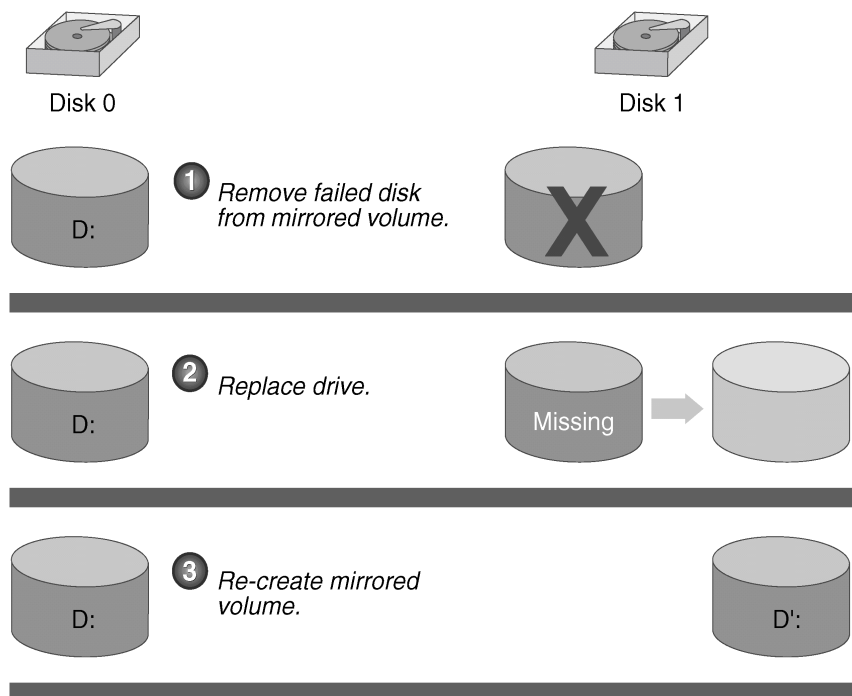
התאוששות מכשל ב-Mirrored Volume

ב-Mirroed Volume, המחשב שומר נתונים בכל חבר בו-זמנית. אם חבר אחד כושל, החבר התקין ממשיך לפעול.

להחלפת חבר שכשל, יש תחילה "להסיר" את הדיסק שכשל מה-Mirrored Volume. באמצעות תוסף התוכנה Computer Management, ניתן לבודד את החבר הפעיל כ-volume נפרד. אז, ניתן להחליף את הדיסק שכשל בדיסק תקין.

ליצירה מחדש של ה-Mirrored Volume לאחר החלפת הדיסק שכשל, לחץ על המחיצה הפעילה בחלון Computer Management, ולחץ Add Mirror. המחשב יציג את האפשרות לבצע Mirror על מחיצה זו אל הדיסק החלופי.

בתרשים 12.14, כונן D בדיסק 0 משוקף בדיסק 1. כונן D בדיסק 1 הוא החבר המשני של ה-Mirrored Volume.



תרשים 12.14 החלפת דיסק שכשל ב-Mirrored Volume.

אם החבר העיקרי ב-Mirrored Volume (זה הכולל את מחיצת האתחול) כושל, השתמש בדיסקט אתחול להפעלת המחשב ולקבלת גישה אל החבר הפעיל. הקובץ Boot.ini בדיסקט האתחול חייב לכלול את הנתיב **A**dvanced **R**ISC **C**omputing (ARC) המצביע אל המחיצה המשופקת. מומלץ ליצור ולבדוק דיסקט אתחול מייד לאחר יישום Mirrored Volume.

הערה החלפת חבר שכשל אינה הסיבה היחידה להסרת Mirrored Volume. **ניתן** גם להסיר חבר אחד ב-Mirrored Volume לניצול שטח הדיסק למטרות אחרות.

תיקון RAID-5 Volume

אם חבר ב-RAID-5 Volume כושל, המחשב ממשיך לפעול עם גישה לכל הנתונים. אולם, כאשר מתבקשים נתונים, Windows 2000 Server fault tolerance driver משתמש בנתונים ובסיביות הנתונים בחברים הנותרים ליצירה מחדש של הנתונים החסרים. יצירת הנתונים החסרים מתבצעת בזיכרון RAM, דבר הגורם להפחתה בביצועי המערכת בעת התהליך.

לשחזור רמת הביצועים של המחשב, ניתן להחליף את הכונן שכשל, ואז לתקן את RAID-5 Volume. Fault Tolerance Driver קורא את מידע הזוגיות מפסי מידע הזוגיות (Parity Information Stripes) בחברים הנותרים, ואז יוצר מחדש את הנתונים שהיו בחבר החסר. בסיום, Fault Tolerance Driver כותב את הנתונים לחבר החדש.

סיכום שיעור

התאוששות מאסון מאפשרת לשחזר מחשב, כך שניתן להיכנס אליו ולגשת למשאבי מערכת לאחר התרחשות אסון מחשב. Windows 2000 כוללת שלוש שיטות המאפשרות לתקן מערכת: **מצב בטוח** (Safe Mode), **חלון ההתאוששות** (Recovery Console), **ודיסק תיקון חירום - ERD** (**E**mergency **R**epair **D**isk). מצב בטוח מאפשר להפעיל את המערכת עם ערכה מינימלית של מנהלי התקנים ושירותים. חלון ההתאוששות מפענח פקודות במצב טקסט, הנפרד ממנחה שורת הפקודה של Windows 2000, ומאפשר למנהל המערכת גישה לדיסק הקשיח של מחשב המפעיל Windows 2000. דיסק תיקון חירום (ERD) מאפשר לשחזר קבצי ליבת המערכת. בנוסף לתיקון המערכת, יש צורך לשחזר נתונים. Windows Backup מספק אשף Restore המסייע בשחזור נתונים, וניתן גם לשחזר את הנתונים ללא האשף. בנוסף, אם המערכת הוגדרה עם Falut tolerance, ניתן להתאושש מכשל ב-Mirrored Volume, או לתקן RAID-5 Volume.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות לשאלה, עיין בשיעור המתאים ונסה לענות על השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואח"כ בעברית.

1. You have configured a computer to boot Windows 2000 Server as the default operating system, and Windows NT 4.0 Server as the optional operating system. After modifying the attributes of files on % systemdrive% and deleting some of the files, the computer does not display Windows NT 4.0 Server as an operating system to start. Windows 2000 Server starts up properly. The problem is caused because you deleted a file. What is the name of the file, and what can you do to recover from this error?
2. You have created three hardware profiles for your mobile computer: Docked, Undocked On The Network, and Undocked At Home. When you reboot the computer, the first two hardware profiles appear, but the third one does not. What is the most likely reason that the Undocked At Home profile is not appearing?
3. Why would the Use Hardware Compression, If Available check box be unavailable in the Backup wizard?
4. You performed a normal backup on Monday. For the remaining days of the week, you only want to back up files and folders that have changed since the previous day. What backup type do you select?
5. How can you test the configuration of the UPS service on a computer?

1. הגדרת מחשב לאתחל את Windows 2000 Server כמערכת ההפעלה של ברירת המחדל, ו- Windows NT 4.0 Server כמערכת הפעלה משנית. לאחר שינוי המאפיינים של קבצים ב- %systemdrive% ומחיקת חלק מהקבצים, המחשב אינו מציג את Windows NT 4.0 Server כמערכת הפעלה אפשרית לאתחול. Windows 2000 Server מופעלת בהצלחה. הבעיה נגרמה כיון שמחקת קובץ כלשהו. מהו שם הקובץ, ומה ניתן לעשות כדי להתאושש מבעיה זו?

2. יצרת שלושה פרופילי חומרה עבור המחשב הנייד שלך: Docked (מעוגן), Undocked On The Network (לא מעוגן אך ברשת), ו- Undocked At Home (לא מעוגן בבית). כאשר מאתחלים את המחשב, יוצגו שני פרופילי החומרה הראשונים, אולם השלישי אינו מוצג. מהי הסיבה הסבירה ביותר לכך שפרופיל Undocked At Home אינו מוצג?

3. מה עשוי להיות הגורם לכך שתיבת הסימון Use Hardware Compression, If Available, אינה זמינה באשף Backup?

4. ביצעת גיבוי רגיל ביום שני. ביתר ימי השבוע, נדרש לגבות רק קבצים ותיקיות שהשתנו מאז היום הקודם. באיזה סוג גיבוי תבחר?

5. כיצד ניתן לבדוק את הגדרות שירות UPS במחשב?

פרק 13

ניטור ומיטוב

אודות פרק זה

Windows 2000 מספקת מערכת כלים ושירותים, המאפשרת ניטור (Monitoring) ומיטוב (Optimization) של המערכת. לדוגמה, ניתן להשתמש בתוסף התוכנה Disk Defragmenter (מאחה הדיסק) לאיתור ואיחוי קבצים ותיקיות מפוצלים ב-local volumes, וניתן להשתמש ב- Network Monitor להצגה ולאיתור בעיות ברשת. פרק זה דן ברבים מהכלים והשירותים המאפשרים ניטור, אבחון תקלות, וביצוע כוונון עדין של המערכת, כולל אותם כלים ושירותים שיכולים לשמש למיטוב ביצועי הדיסק והרשת.

לפני שתתחיל

לביצוע השיעורים בפרק זה, נדרש:

- ❖ Server01 המפעיל Windows 2000 Server.
- ❖ השלמת התרגילים בפרקים הקודמים.

שיעור 1: ניטור ומיטוב דיסק

Windows 2000 כוללת מספר כלים בהם ניתן להשתמש לאבחון בעיות בדיסק, לשיפור ביצועים, ולדחיסת נתונים. בין כלים אלה ניתן למצוא את Check Disk, תוסף התוכנה Disk Defragmenter, דחיסת נתונים וניהול מכסות שטח דיסק. שיעור זה דן בכל אחד מכלים אלה, ומציג כיצד משתמשים בהם. שיעור 2 חוקר את נושא ניטור הדיסק, בהקשר של ניטור ביצועי מערכת.

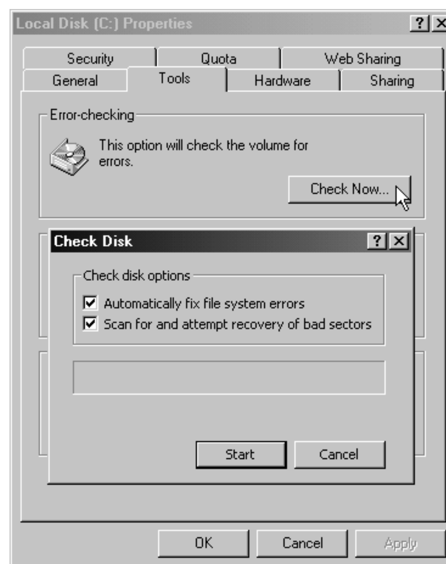
לאחר שיעור זה, תוכל

- להשתמש ב- Check Disk, בתוסף התוכנה Disk Defragmenter, בדחיסת נתונים ובמכסות שטח דיסק, למיטוב ביצועי הדיסק.

זמן לימוד משוער: 40 דקות

Check Disk

הכלי Check Disk, המכונה גם **כלי לבדיקת שגיאות**, מאפשר לבדוק שגיאות במערכת הקבצים וסקטורים פגומים בדיסק הקשיח. לשימוש ב-Check Disk, פתח את תיבת הדו-שיח Properties עבור הדיסק המסוים שברצונך לבדוק. ניתן לפתוח את תיבת הדו-שיח Properties מתוך סייר Windows או מתוך My Computer. בכרטיסיה Tools, לחץ על Check Now לפתיחת תיבת הדו-שיח Check Disk ובחר את האפשרויות המתאימות (תרשים 13.1).



תרשים 13.1 תיבת הדו-שיח Check disk, שנפתחה באמצעות הכרטיסיה Tools שבתיבת הדו-שיח Properties.

יש לסגור את כל היישומים הפעילים או הקבצים הפתוחים בדיסק הנבדק, כדי שהליך Check Disk יוכל לתקן אוטומטית שגיאות במערכת הקבצים. אם קבצים כלשהם פתוחים או שיישומים פועלים, תוצג תיבת הודעה, בה נכתב כי לא ניתן להשיג גישה בלעדית לכונן, ואתה נשאל האם ברצונך לתזמן מחדש את בדיקת הדיסק לפעם הבאה בה תפעיל את המחשב.

אם volume מפורמט עם מערכת קבצים NT (NTFS), אז Windows 2000 רושמת את כל פעולות הקבצים, מחליפה אשכולות פגומים אוטומטית, ומאחסנת עותקים של מידע מפתח עבור כל הקבצים ב-NTFS volume.

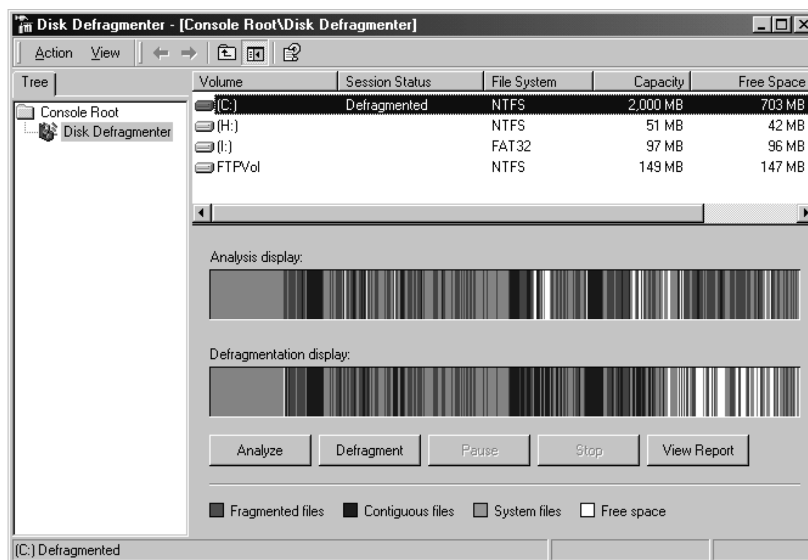
תוסף התוכנה Disk Defragmenter

Windows 2000 שומרת קבצים ותיקיות במקום הפנוי הראשון בדיסק קשיח ולא בהכרח באזור של מרווח רציף. הדבר מוביל לפיצול (Fragmentation) קבצים ותיקיות. כאשר הדיסק הקשיח מכיל הרבה קבצים ותיקיות מפוצלים, נדרש למחשב זמן רב יותר לגשת אליהם, כיון שנדרשות קריאות רבות נוספות לאיסוף החלקים השונים. יצירת קבצים ותיקיות חדשים דורשת אף היא זמן רב יותר, כיון שהמקום הפנוי בדיסק הקשיח מפוזר. על המחשב לשמור קובץ או תיקיה חדשים במספר מיקומים על הדיסק הקשיח.

Defragmenting Disks

הליך מציאת ואיחוד קבצים ותיקיות מפוצלים נקרא **איחוי** (Defragmenting). תוסף התוכנה Disk Defragmenter משמש לאיתור קבצים ותיקיות מפוצלים, ואז הוא מאחה אותם. הוא פועל על ידי העברת החלקים של כל קובץ או תיקיה למיקום אחד, כך שכל קובץ או תיקיה תופש אזור יחיד של שטח רציף על הדיסק הקשיח. בעקבות זאת, המערכת יכולה לגשת ולשמור קבצים ותיקיות ביעילות רבה יותר. על ידי איחוי קבצים ותיקיות תוסף התוכנה Disk Defragmenter גם מאחד את השטח הפנוי, וכך מקטין את הסיכוי שקבצים חדשים יהיו מפוצלים. Disk Defragmenter מאחה את ה-volumes במבנה FAT16, FAT32 ו-NTFS.

ניתן לגשת לתוסף התוכנה Disk Defragmenter דרך תוסף התוכנה Computer Management, או על ידי יצירת MMC Console מותאם אישית המכיל את תוסף התוכנה Disk Defragmenter. כאשר Disk Defragmenter נבחר, חלונית הפרטים מפוצלת לשלושה אזורים, כמתואר בתרשים 13.2. ניתן גם לגשת לתוסף התוכנה Disk Defragmenter באמצעות סייר Windows או My Computer על ידי פתיחת תיבת הדו-שיח Properties עבור הכונן המסוים. בכרטיסיה Tools, לחץ על Defragment Now.



תרשים 13.2 תוסף התוכנה Disk Defragmenter, בגישה באמצעות MMC console מותאם אישית.

החלק העליון של החלון מציג רשימה של ה-volumes שאותם ניתן לנתח ולאחות. החלק האמצעי הוא תצוגה גרפית של מידת הפיצול של ה-volume שנבחר. החלק התחתון הוא תצוגה דינמית של ה-volume המעודכן בעת במהלך האיחוי.

צבעי התצוגה מציינים את מצב המחיצה:

- אדום מציין קבצים מפוצלים.
- כחול כהה מציין קבצים רציפים (לא מפוצלים).
- לבן מציין מקום פנוי ב-volume.
- ירוק מציין קבצי מערכת, אותם Disk Defragmenter אינו יכול להזיז.

על ידי השוואת פס הצגת הניתוח מול פס הצגת האיחוי, בעת האיחוי ובסיומו, ניתן לראות בקלות את השיפור ב-volume.

לניתוח או איחוי volume, ניתן לבחור אחת מהאפשרויות המתוארות בטבלה הבאה.

אפשרות	תיאור
Analyze	**לחץ על לחצן זה לביצוע ניתוח של הדיסק המיועד לאיחוי. לאחר הניתוח, תספק הצגת הניתוח** (Analysis display) **תצוגה גרפית של מידת הפיצול של הקבצים ב-volume.**
Defragment	**לחץ על לחצן זה לביצוע איחוי של הדיסק. לאחר האיחוי, תציג תצוגת האיחוי** (Defragmentation display) **תצוגה גרפית של ה-volume לאחר האיחוי.**

שימוש יעיל במאחה הדיסק

הרשימה הבאה מציגה הנחיות לשימוש בתוסף התוכנה Disk Defragmenter.

- הפעל את Disk Defragmenter כאשר השימוש במחשב מינימלי. בעת האיחוי, נתונים מועברים ממקום למקום על הדיסק הקשיח. הליך האיחוי צורך פעילות רבה של המעבד (CPU), ועלול להשפיע לרעה על זמן הגישה למשאבים אחרים מבוססי-דיסק.
- המלץ למשתמשים לאחות את הדיסקים המקומיים שלהם לפחות פעם בחודש, למניעת הצטברות קבצים מפוצלים.
- נתח את ה-volume המיועד לפני התקנת יישומים גדולים, ואז אחה את ה-volume לפי הצורך. התקנות מתבצעות מהר יותר כאשר אמצעי היעד מכיל מספיק שטח פנוי רציף. בנוסף, הגישה ליישום תהיה מהירה יותר לאחר התקנתו.
- כאשר מוחקים מספר רב של קבצים או תיקיות, הדיסק הקשיח עשוי להיות מפוצל במידה רבה, לכן כדאי לנתח אותו ולאחות לפי הצורך. באופן כללי, כדאי לאחות דיסקים על שרתי קבצים עמוסים לעתים קרובות יותר מאשר דיסקים במחשבי לקוח בעלי משתמש יחיד.
- כדאי לשקול שימוש בתוכנית שירות לאיחוי דיסק המאפשרת לבצע איחוי דיסק מתוזמן בכל הרשת ממיקום מרכזי. Executive Software יצרה את ה-Disk Defragmenter הידני הנכלל ב-Windows 2000 ומייצרת גירסה אוטומטית, עשירה יותר בתכונות, של תוכנית שירות זו כמוצר נפרד הנקרא Diskeeper.

הערה למידע נוסף אודות Executive Software Diskeeper 5.0, בקר באתר האינטרנט של החברה בכתובת http://www.execsoft.com.

דחיסת נתונים

דחיסת נתונים מאפשרת לדחוס קבצים ותיקיות ב-NTFS volumes. קבצים ותיקיות דחוסים תופסים פחות מקום ב-NTFS-formatted volume, דבר המאפשר אחסון יותר נתונים. מצב הדחיסה עבור כל קובץ ותיקיה ב- NTFS volume מוגדר לדחיסה או אי-דחיסה.

שימוש בקבצים ותיקיות דחוסים

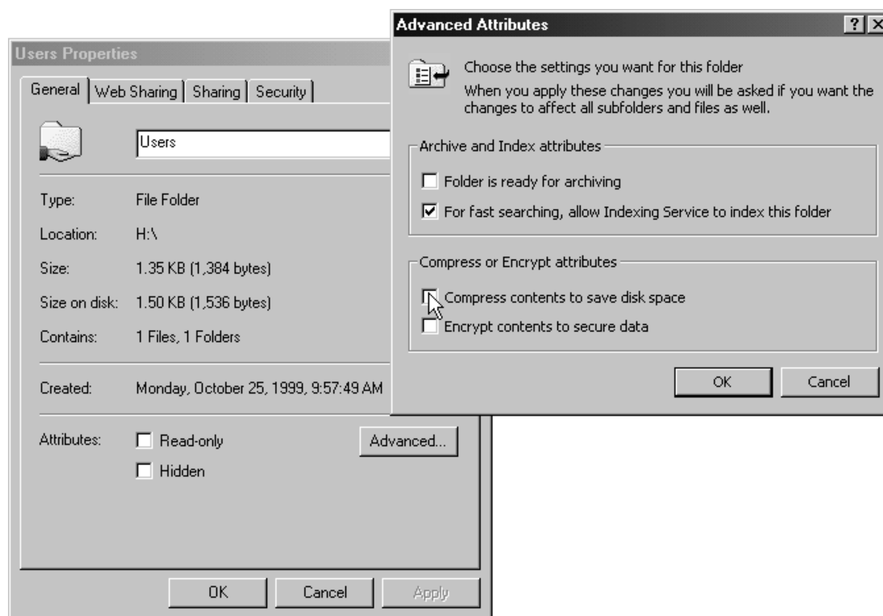
קבצים דחוסים ניתנים לקריאה ולכתיבה לכל יישום מבוסס Windows או MS-DOS, ללא צורך בפתיחת הדחיסה תחילה על ידי תוכנית אחרת. כאשר יישום, כגון מעבד תמלילים Word, או פקודת מערכת הפעלה, כגון Copy, מבקשים גישה לקובץ דחוס, NTFS פותחת אוטומטית את הדחיסה של הקובץ לפני הצגתו כזמין. כאשר סוגרים או שומרים קובץ, NTFS דוחסת אותו שוב.

NTFS מקצה מקום בדיסק על סמך גודל הקובץ כאשר אינו דחוס. אם מעתיקים קובץ דחוס אל NTFS volume עם מספיק מקום עבור הקובץ הדחוס, אך לא מספיק עבור הקובץ שאינו דחוס, תוצג הודעת שגיאה שאין מספיק מקום בדיסק עבור הקובץ. הקובץ לא יועתק ל-volume.

דחיסת קבצים ותיקיות

ניתן להגדיר את מצב הדחיסה של קבצים ותיקיות בעזרת סייר Windows, או על ידי שימוש בתוכנית השירות Compact משורת הפקודה. למידע אודות תחביר תוכנית השירות Compact, עבור לשורת הפקודה והקלד **Compact /?**.

לדחיסת קובץ או תיקיה, פתח את תיבת הדו-שיח Properties עבור הקובץ או התיקיה הרצויים. בכרטיסיה General, לחץ Advanced. בתיבת הדו-שיח Advanced Attributes, סמן את תיבת הסימון Compress Contents To Save Disk Space, כמתואר בתרשים 13.3. שים לב שהצפנה ודחיסה של NTFS אינם חופפים, אם בוחרים את תיבת הסימון Encrypt Contents To Secure Data, לא ניתן לדחוס קובץ או תיקיה זו.



תרשים 13.3 תיבת הדו-שיח Advanced Attributes (מאפיינים מתקדמים).

ניתן גם להגדיר דחיסה עבור הכונן כולו. כדי לעשות זאת, פתח את תיבת הדו-שיח Properties עבור הכונן הרצוי. בכרטיסיה General, סמן את תיבת הסימון Compress Drive To Save Disk Space.

לשינוי מצב הדחיסה עבור קובץ או תיקיה, יש צורך בהרשאות כתיבה (Write) עבורם.

דגל הדחיסה עבור תיקיה אינו משקף את מצב הדחיסה של הקבצים בתיקיה זו ותיקיות המשנה. תיקיה יכולה להיות מסומנת כך שקבצים שיוספו מאוחר יותר יהיו דחוסים, אולם כל הקבצים הנמצאים כעת בתיקיה יישארו לא דחוסים. בנוסף, תיקיה שאינה מסומנת בדגל הדחיסה יכולה להכיל גם קבצים דחוסים. כאשר בוחרים באפשרות דחיסת תיקיה ואז לוחצים על Apply או OK בתיבת הדו-שיח Properties, Windows 2000 מציגה את תיבת הדו-שיח Confirm Attribute Changes, שבה יש שתי אפשרויות נוספות. אפשרויות אלו מתוארות בטבלה הבאה.

אפשרות	תיאור
Apply changes to this folder only	דוחס את הקבצים בתיקיה שנבחרה בלבד.
Apply changes to this folder, subfolders and files	דוחס את הקבצים בתיקיה, מסמן תת-תיקיות בדגל הדחיסה, ודוחס קבצים בתת-התיקיות וקבצים המתוספים מאוחר יותר.

הערה Windows 2000 אינה תומכת בדחיסת NTFS עבור גדלי אשכול מעל 4KB, מכיון שדחיסה באשכולות גדולים גורמת לפגיעה בביצועים. אם בוחרים גודל אשכול גדול יותר כאשר מפרמטים NTFS volume, הדחיסה אינה זמינה עבור volume זה.

בחירת צבע תצוגה חלופי עבור קבצים ותיקיות דחוסים

סייר Windows מקל על הבחנה מהירה בקובץ או תיקיה דחוסים, על ידי מתן אפשרות לבחור צבע תצוגה שונה עבור קבצים ותיקיות דחוסים. בדרך זו ניתן להבדיל ביניהם לבין קבצים ותיקיות שאינם דחוסים.

להגדרת צבע תצוגה חלופי עבור קבצים ותיקיות דחוסים, בחר Folder Options מתפריט Tools. בכרטיסיה View, סמן את תיבת הסימון Display Compressed Files And Folders With Alternate Color. תיקיות וקבצים דחוסים יופיעו בצבע כחול. אין אפשרות לבחור בצבע שונה.

העתקה והעברה של קבצים ותיקיות דחוסים

קיימים חוקים הקובעים האם מצב הדחיסה של קבצים ותיקיות נשמר, כאשר מעתיקים או מעבירים אותם בתוך ובין NTFS volumes ו-FAT volumes. הסעיפים הבאים מתארים כיצד Windows 2000 מתייחסת למצב הדחיסה של קובץ או תיקיה דחוסים, כאשר מעתיקים או מעבירים אותם בתוך או בין NTFS volumes או בין NTFS volumes ל-FAT volumes.

העתקת קובץ בתוך NTFS volume

כאשר מעתיקים קובץ בתוך NTFS volume, יורש הקובץ את מצב הדחיסה של תיקיית היעד. לדוגמה, אם מעתיקים קובץ דחוס לתיקיה שאינה דחוסה, הקובץ נפרש אוטומטית.

העברת קובץ או תיקיה בתוך NTFS volume

כאשר מעבירים קובץ או תיקיה בתוך NTFS volume, הקובץ או התיקיה שומרים על מצב הדחיסה המקוריים שלהם. לדוגמה, אם מעבירים קובץ דחוס לתיקיה שאינה דחוסה, הקובץ נותר דחוס.

העתקת קובץ או תיקיה בין NTFS volumes

כאשר מעתיקים קובץ או תיקיה בין NTFS volumes, הקובץ או התיקיה יורשים את מצב הדחיסה של תיקיית היעד.

העברת קובץ או תיקיה בין NTFS volumes

כאשר מעבירים קובץ או תיקיה בין NTFS volumes, הקובץ או התיקיה יורשים את מצב הדחיסה של תיקיית היעד. כיון ש-Windows 2000 מתייחסת להעברה כאל העתקה ואז מחיקה, הקבצים יורשים את מצב הדחיסה של תיקיית היעד.

העברה או העתקה של קובץ או תיקיה ל-FAT volume

Windows 2000 תומכת בדחיסה עבור קבצי NTFS בלבד. לכן, כאשר מעבירים או מעתיקים קובץ או תיקיית NTFS דחוסים ל-FAT volume, Windows 2000 פורשת אוטומטית את הקובץ או התיקיה.

העברה או העתקה של קובץ או תיקיה דחוסים לדיסקט

כאשר מעבירים או מעתיקים קובץ או תיקיית NTFS דחוסים לדיסקט, Windows 2000 פורשת אוטומטית את הקובץ או התיקיה.

הערה כאשר מעתיקים קובץ NTFS דחוס, Windows 2000 פורשת את הקובץ, מעתיקה אותו, ואז, אם תיקיית היעד מסומנת לדחיסה, דוחסת את הקובץ שוב כקובץ חדש. פעולות אלו עלולות לגרום לפגיעה בביצועים.

שימוש בדחיסת NTFS

להלן רשימה של פעולות שיסייעו בדחיסה טובה ב-NTFS volumes.

- כיון שקבצים מסוגים מסוימים נדחסים יותר מאחרים, בחר סוגי קבצים לדחיסה על סמך גודל הקובץ הדחוס הצפוי. לדוגמה, כיון שקבצי מפת סיביות של Windows (BMP) מכילים יותר נתונים יתירים (Redundant Data) מאשר קבצי הפעלה של יישומים, סוג קובץ זה נדחס לגודל קטן יותר. קובץ BMP נדחס במקרים רבים לפחות מרבע גודל הקובץ המקורי, בעוד שקבצי יישומים רק לעתים רחוקות נדחסים לפחות מ- 75 אחוזים מהגודל המקורי.
- אל תאחסן קבצים דחוסים, כגון קבצי ZIP, בתיקיה דחוסה. Windows 2000 תנסה לדחוס את הקובץ, וכך תבזבז זמן מערכת ללא פינוי שטח נוסף בדיסק.
- כדי להקל על איתור נתונים דחוסים, השתמש בצבע תצוגה שונה עבור קבצים ותיקיות דחוסים.

- דחוס נתונים סטטיים, ולא נתונים המשתנים לעתים קרובות. דחיסה ופרישה של קבצים יוצרות תקורה מסוימת של המערכת. על ידי בחירה לדחוס קבצים שאינם בשימוש לעתים קרובות, מפחיתים את כמות זמן המערכת המוקדש לפעולות דחיסה ופרישה.
- דחיסת NTFS עשויה לגרום לפגיעה בביצועים כאשר מעתיקים ומעבירים קבצים. כאשר קובץ דחוס מועתק לתיקיה אחרת המסומנת לדחיסה, הוא נפרש, מועתק, ואז נדחס שוב כקובץ חדש.

Disk Quotas

ניתן להשתמש במכסות שטח דיסק (Disk Quotas) לניהול גידול באחסון בסביבות מבוזרות. מכסות שטח דיסק מאפשרות להקצות שימוש בשטח דיסק למשתמשים, על סמך הקבצים והתיקיות שבבעלותם. ניתן להגדיר מכסות שטח דיסק, סף מכסה (Quota Threshold), וגבולות מכסה (Quota Limits) עבור כל המשתמשים, ועבור משתמשים מסוימים. ניתן גם לעקוב אחר כמות השטח על הדיסק הקשיח בו השתמשו משתמשים, והכמות שנותרה להם מול המכסה שלהם.

ניהול מכסות שטח דיסק

Disk Quotas של Windows 2000 עוקבות ושולטות על שימוש בדיסק per-user, per-volume. Windows 2000 עוקבת אחר מכסות שטח דיסק עבור כל volume, גם אם volumes נמצאים באותו דיסק קשיח. כיון שמעקב מכסות מתבצע לפי-משתמש, שטח הדיסק של כל משתמש מבוקר ללא תלות בתיקיה בה המשתמש שומר קבצים. כלי ניהול מכסות שטח דיסק מגורם שלישי מספקים יכולות ניהול מכסות פרטנית, כמו מעקב אחר שימוש בדיסק על בסיס לפי- משתמש, לפי-תיקיה.

הרשימה הבאה מתארת מספר מאפיינים חשובים של מכסות שטח דיסק ב- Windows 2000.

- Windows 2000 מחשבת שימוש בשטח דיסק עבור משתמשים על סמך הקבצים והתיקיות שבבעלותם. כאשר משתמש מעתיק או שומר קובץ חדש ל-NTFS volume או לוקח על עצמו בעלות על קובץ ב-NTFS volume, Windows 20000 מחייבת את שטח הדיסק עבור הקובץ מול גבול המכסה של המשתמש.
- Windows 2000 מתעלמת מדחיסה, כשהיא מחשבת שימוש בשטח דיסק קשיח. משתמשים מחויבים עבור כל בית לא דחוס, ללא תלות בשטח הדיסק הקשיח שבשימוש בפועל. חלקית, חיוב זה מבוצע כיון שדחיסת קבצים יוצרת רמות דחיסה שונות עבור סוגי קבצים שונים. סוגי קבצים שונים, שהם בעלי גודל זהה כאשר אינם דחוסים, עשויים להיות בעלי גדלים שונים לחלוטין לאחר דחיסתם.

- כאשר מפעילים מכסות שטח דיסק, השטח הפנוי ש-Windows 2000 מדווחת ליישומים עבור הקובץ, הוא כמות המקום הפנוי שנשאר בתוך גבול מכסת שטח הדיסק של המשתמש. לדוגמה, משתמש שהקבצים שלו תופסים 50MB מתוך הקצאת גבול מכסת שטח דיסק של 100MB, יציג 50MB של מקום פנוי גם אם יש ב-volume יש מספר GB שטח פנוי.

הערה ניתן להחיל מכסות שטח דיסק רק על Windows 2000 NTFS volumes.

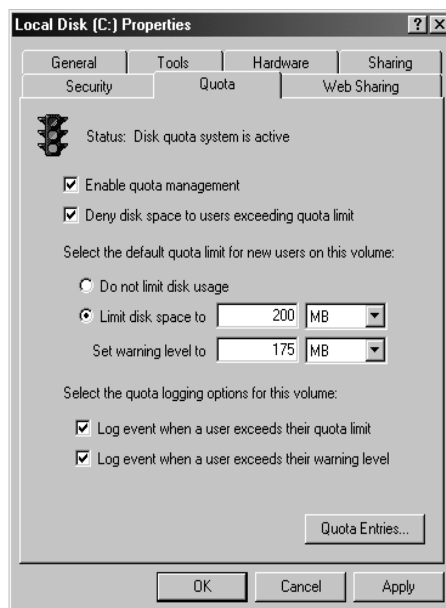
ניתן להשתמש במכסות שטח דיסק לבקרה ושליטה על שימוש בשטח בדיסק קשיח. מנהלי מערכות יכולים לבצע את הפעולות הבאות:

- הגדרת גבול מכסת שטח דיסק (Quota), שיציין את כמות שטח הדיסק עבור כל משתמש.
- הגדרת אזהרת מכסות שטח דיסק שתציין מתי Windows 2000 תרשום אירוע, המציין שהמשתמש מתקרב לגבול המוקצה לו.
- אכיפת גבולות מכסת שטח דיסק ומניעת גישה למשתמשים, אם הם חורגים מהגבול שלהם, או אפשור המשך גישה.
- רישום אירוע, כאשר משתמש חורג מסף שטח דיסק מסוים. לדוגמה, סף עשוי להיות כשמשתמשים חורגים מגבול המכסה שלהם, או כאשר הם חורגים מרמת האזהרה שלהם.

לאחר אפשור מכסות שטח דיסק עבור volume מסויים, Windows 2000 אוספת נתוני שימוש בדיסק עבור כל המשתמשים שבבעלותם קבצים ותיקיות ב-volume זה. הדבר מאפשר מעקב אחר השימוש ב-volume לפי-משתמש. כברירת מחדל, רק חברים בקבוצת Administrators יכולים להציג ולשנות הגדרות מכסות. אולם, ניתן לאפשר למשתמשים להציג הגדרות מכסות.

הגדרת מכסות שטח דיסק

ניתן לאפשר מכסות שטח דיסק ולאכוף אזהרות וגבולות מכסות שטח דיסק עבור כל המשתמשים או עבור משתמשים מסוימים. כדי לאפשר מכסות שטח דיסק, פתח את תיבת הדו-שיח Properties של דיסק מסוים, בחר בכרטיסיה Quota, והגדר את אפשרויות Disk Quota הרצויות (תרשים 13.4).



תרשים 13.4 הכרטיסיה Quota בתיבת הדו-שיח Properties של דיסק.

האפשרויות בכרטיסיה Quota מתוארות בטבלה הבאה:

אפשרות	תיאור
Enable Quota Management	סמן תיבת סימון זו כדי להפעיל ניהול מכסות
Deny Disk Space To Users Exceeding Quota Limit	סמן תיבת סימון זו כך, שכאשר משתמשים חורגים מהקצאת המקום שלהם בדיסק הקשיח, הם יקבלו הודעת "אין מקום בדיסק" ולא יוכלו לכתוב ל-volume זה.
Do Not Limit Disk Usage	לחץ על אפשרות זו, כאשר לא רוצים להגביל את כמות השטח בדיסק הקשיח עבור משתמשים.
Limit Disk Space To	הגדר את כמות שטח הדיסק, שבה מותר למשתמשים להשתמש.
Set Warning Level To	הגדר את כמות שטח הדיסק שמשתמש יכול למלא לפני ש- Windows 2000 רושמת אירוע, המציין שהמשתמש מתקרב לגבול שהוקצה לו.
Quota Entries	לחץ על לחצן זה לפתיחת Quota Entries עבור תיבת דו-שיח, שם ניתן להוסיף רישום חדש, למחוק רישום קיים, ולהציג את מידע המכסה לפי-משתמש.

כדי לאכוף גבולות מכסה זהים עבור כל המשתמשים, הזן את הערכים המתאימים בתיבת הטקסט Limit Disk Space To, ובתיבת הטקסט Set Warning Level To, ואז סמן את תיבת הסימון Deny Disk Space To Users Exceeding Quota Limit.

Windows 2000 עוקבת אחר שימוש ולא תאפשר למשתמשים ליצור קבצים או תיקיות ב-volume כאשר הם חורגים מהגבול.

קביעת המצב של מכסות שטח דיסק

ניתן לקבוע את המצב של מכסות שטח דיסק בתיבת הדו-שיח Properties עבור דיסק על ידי בדיקת סמל הרמזור וקריאת הודעת המצב מימינו (תרשים 13.4). צבעי הרמזור והמצב שהם מציינים הם:

- ❖ רמזור אדום מציין שמכסות שטח דיסק אינן מופעלות.
- ❖ רמזור צהוב מציין ש-Windows 2000 בונה מחדש את מידע מכסות שטח הדיסק.
- ❖ רמזור ירוק מציין שמערכת מכסות שטח דיסק פעילה.

אכיפת מכסות שטח דיסק

לאכיפת גבולות מכסה שונים עבור משתמש מסוים או מספר משתמשים, לחץ על הלחצן Quota Entries לפתיחת תיבת הדו-שיח Quota Entries. הגדר את גבול שטח הדיסק ואת רמת האזהרה עבור כל משתמש.

ניתן להשתמש בתיבת הדו-שיח Quota Entries For <volume_name> למעקב אחר השימוש עבור כל המשתמשים שהעתיקו, שמרו, או קיבלו על עצמם בעלות על קבצים ותיקיות ב-volume. Windows 2000 סורקת את ה-volume, ועוקבת אחר כמות שטח הדיסק שבשימוש על ידי כל משתמש. תיבת הדו-שיח Quota Entries For <volume_name> מאפשרת להציג את המידע הבא:

- ❖ כמות שטח הדיסק הקשיח בו משתמש כל משתמש.
- ❖ משתמשים הנמצאים מעל סף אזהרת המכסה שלהם, אשר מצוין על ידי משולש צהוב.
- ❖ משתמשים החורגים מגבול המכסה שלהם, המצוין על ידי עיגול אדום.
- ❖ סף האזהרה וגבול מכסה עבור כל משתמש.

נעשה מעקב אחר שימוש ב-volume לכל המשתמשים שבבעלותם קבצים ב-volume שבה מערכת Disk Quota פעילה. משתמשים קיימים שהם בעלי קבצים, מוגבלים לברירות המחדל של מכסות שטח דיסק אלא אם משנים את הגדרת המכסה של המשתמש באמצעות תיבת הדו-שיח Quota Entries For <volume_name>. משתמשים שאין להם קבצים ב-volume, לא יוצגו בתיבת הדו-שיח Quota Entries For <volume_name>, אולם ניתן להוסיפם ידנית. כברירת מחדל, גבולות מכסה אינם מוחלים על הקבוצה המקומית Administrators.

שימוש מיטבי במכסות שטח דיסק

להלן רשימת הנחיות לשימוש במכסות שטח דיסק:

- ❖ אם מאפשרים הגדרות מכסה ב-volume בו מותקנת Windows 2000, ולחשבון המשתמש שלך יש גבול מכסה, עליך להיכנס בשם משתמש Administrator להתקנת רכיבים ויישומים נוספים של Windows 2000. כאשר תעשה זאת, Windows 2000 לא תחייב את שטח הדיסק בו תשתמש להתקנת יישומים כחלק מהקצבת מכסת שטח הדיסק בחשבון המשתמש שלך.
- ❖ ניתן לבקר שימוש בדיסק קשיח ולהפיק מידע שימוש בדיסק קשיח, מבלי למנוע ממשתמשים לשמור נתונים. כדי לעשות זאת, נקה את תיבת הסימון Deny Disk Space To Users Exceeding Limit בעת אפשור מכסות שטח דיסק.
- ❖ הגדר גבולות ברירת מחדל מגבילים יותר עבור כל חשבונות המשתמשים, ואז שנה את הגבולות מתיבת הדו-שיח Quota Entries For <volume_name>, כדי לאפשר שטח דיסק נוסף למשתמשים העובדים עם קבצים גדולים.
- ❖ באופן כללי, כדאי להגדיר מכסות שטח דיסק על shared volumes, להגבלת שטח האחסון עבור משתמשים. הגדר מכסות שטח דיסק בתיקיות ציבוריות ובשרתי רשת, כדי להבטיח שמשתמשים ישתפו שטח דיסק קשיח באופן מתאים. כאשר יש מחסור במשאבי אחסון, כדאי להגדיר מכסות שטח דיסק על כל השטח המשותף בדיסקים קשיחים.
- ❖ מחק רישומי מכסה עבור משתמשים שאינם מאחסנים עוד את הקבצים שלהם ב-volume. ניתן למחוק רישומי Quota עבור חשבון משתמש, רק לאחר שכל הקבצים שבבעלות משתמש זה הוסרו מה-volume, או שמשתמש אחר לקח על עצמו בעלות על הקבצים.
- ❖ לפני שניתן למחוק רישום מכסה עבור חשבון משתמש, כל הקבצים שבבעלות משתמש זה חייבים להיות מוסרים מה-volume, או שמשתמש אחר חייב לקחת בעלות על הקבצים. דרך יעילה להסרת קבצים של משתמש או לקחת בעלות עליהם למטרה זו היא למחוק את חשבון המשתמש בתיבת הדו-שיח Quota Entries For <volume_name>. מערכת ניהול Disk Quota תציג את תיבת הדו-שיח Disk Quota. מתיבת דו-שיח זו ניתן לקחת בעלות, למחוק או להעביר את הקבצים.

תרגיל 1: יישום מכסות שטח דיסק

בתרגיל זה, תקבע הגדרות ברירת מחדל לניהול מכסות שטח דיסק, להגבלת כמות הנתונים שמשתמשים יכולים לאחסן בכונן C של Server01. כונן C של Server01 מכיל את שיתוף HomeDirs, שיצרת עבור המשתמש John Smith לאחסון הקבצים שלו. אז, תגדיר הגדרת מכסה מותאמת אישית עבור חשבון משתמש. תגדיל את כמות הנתונים שמשתמש יכול לאחסן על כונן C ל- 20MB עם רמת אזהרה שתוגדר ב- 16MB. לסיום, תכבה ניהול מכסות עבור כונן C. בצע תרגיל זה על Server01.

הליך 1: הגדרת הגדרות ניהול מכסה

בהליך זה, תקבע הגדרות ניהול מכסה עבור כונן C, להגבלת הנתונים שמשתמשים יכולים לאחסן ב-volume.

1. היכנס ל- Server01 בשם משתמש Administrator עם הסיסמה password.
2. בשולחן העבודה, לחץ לחיצה כפולה על My Computer.
3. לחץ על סמל (:Local Disk (C, פתח את תפריט File, ולחץ על Properties.

   Windows 2000 תציג את תיבת הדו-שיח Local Disk (C:) Properties, כאשר הכרטיסיה General פעילה.
4. בחר בכרטיסיה Quota. שים לב שכברירת מחדל מכסות שטח דיסק אינן מופעלות.
5. בכרטיסיה Quota, לחץ על תיבת הסימון Enable Quota Management.
6. לחץ על לחצן אפשרויות Limit Disk Space To.
7. הקלד **10** בתיבת הטקסט Limit Disk Space To, ואז הקלד **6** בתיבת הטקסט Set Warning Level To.

   שים לב שהיחידות של ברירת המחדל הן KB.
8. שנה את גודל היחידות ל-MB, ולחץ Apply.

   תופיע תיבת דו-שיח Disk Quota, ובה אזהרה שתבוצע סריקה מחדש של ה-volume, לעדכון סטטיסטיקת שימוש בדיסק, אם תפעיל מכסות.
9. לחץ OK להפעלת מכסות שטח דיסק.
10. אל תסגור את תיבת הדו-שיח Local Disk (C:) Properties; היא תשמש אותך בהליך הבא.

הליך 2: יצירת הגדרה של מכסה מותאמת אישית עבור משתמש

בהליך זה, תגדיר הגדרת מכסה מותאמת אישית עבור חשבון המשתמש John Smith.

1. בכרטיסיה Quota של תיבת הדו-שיח Local Disk (C:) Properties, לחץ על הלחצן Quota Entries.

   Windows 2000 תציג את תיבת הדו-שיח Quota Entries For Local Disk (C:). שים לב שרשומים חשבונות המשתמשים שיצרת, NT AUTHORITY\SYSTEM, ו-BUILTIN\Administrators. חשבונות המשתמשים שיצרת רשומים, מכיון שלכל שלושת המשתמשים (Jane_Doe, John_Smith ו-Bob_Train) יש קבצים ב-volume זה.

2. בתיבת הדו-שיח Quota Entries For Local Disk (C:), לחץ לחיצה כפולה על השורה המכילה את John Smith. תופיע תיבת הדו-שיח Quota Settings For John Smith.
3. הגדל את כמות הנתונים המותרת ל- John Smith לאחסון על כונן C, על ידי שינוי הערך בתיבה Limit Disk Space To ל- 20MB, ושינוי הערך בתיבה Set Warning Level To ל- 16MB.
4. לחץ OK לחזרה לתיבת הדו-שיח Quota Entries For Local Disk (C:).
5. סגור את תיבת הדו-שיח Quota Entries For Local Disk (C:).
6. השאר את תיבת הדו-שיח Local Disk (C:) Properties פתוחה, היא תשמש אותך בהליך הבא.

הליך 3: ביטול ניהול מכסות

בהליך זה, תבטל הגדרות ניהול מכסות עבור כונן C.

1. בכרטיסיה Quota, נקה את תיבת הסימון Enable Quota Management.

   שים לב שכל הגדרות המכסות עבור כונן C אינן זמינות עוד.

2. לחץ Apply. תופיע תיבת הודעה Disk Quota, ובה אזהרה שאם תבטל מכסות, תבוצע סריקה מחדש של ה-volume אם תפעיל אותן שוב מאוחר יותר.
3. לחץ OK לסגירת תיבת הדו-שיח Disk Quota.
4. לחץ OK לסגירת תיבת הדו-שיח Local Disk (C:) Properties.
5. סגור את החלון My Computer.

סיכום שיעור

Windows 2000 כוללת מספר כלים, בהם ניתן להשתמש לאבחון בעיות בדיסק, לשיפור ביצועים, או לדחיסת נתונים. הכלי Check Disk, המכונה גם כלי לבדיקת שגיאות, מאפשר לבדוק שגיאות במערכת הקבצים ולאתר סקטורים פגומים בדיסק. תוסף התוכנה Disk Defragmenter מאפשר לאתר קבצים ותיקיות מפוצלים, ואז לאחות אותם. הוא עושה זאת על ידי העברת החלקים של כל אחד מהקבצים למיקום יחיד, כך שכל קובץ או תיקיה תופסים אזור יחיד של שטח רציף על הדיסק הקשיח. דחיסת נתונים מאפשרת לדחוס קבצים ותיקיות ב-NTFS volumes. ניתן לקרוא ולכתוב אל קבצים דחוסים בעזרת כל יישום מבוסס Windows או מבוסס MS-DOS, בלי לפתוח אותם תחילה באמצעות תוכנית אחרת. Disk Quotas מאפשרות להקצות שימוש בשטח דיסק למשתמשים על סמך הקבצים והתיקיות שבבעלותם. ניתן להגדיר מכסות שטח דיסק, סף מכסה, וגבול מכסה עבור כל המשתמשים ועבור משתמשים מסוימים. מכסות שטח דיסק שולטות על שימוש בדיסק לפי משתמש (per-user) ו/או per-volume.

שיעור 2: SNMP
(Simple Network Management Protocol)

כדי לעמוד באתגרים של תכנון פלטפורמת ניהול רשת יעילה עבור רשתות הטרוגניות המבוססות על TCP/IP, הוגדר בשנת 1988 פרוטוקול SNMP (**S**imple **N**etwork **M**anagement **P**rotocol). פרוטוקול זה אושר כתקן עבור האינטרנט בשנת 1990, על ידי **I**nternet **A**ctivities **B**oard (IAB). SNMP מאפשר ניטור ותקשור מצב מידע מסוכני SNMP אל תחנת ניהול רשת NMS (**N**etwork **M**anagement **S**tation). שיעור זה מספק את הרקע והחומר הרעיוני הדרושים להבנה ויישום SNMP בהקשר של Windows 2000.

לאחר שיעור זה, תוכל

- להבין את המטרה והפעולה של שירות SNMP.

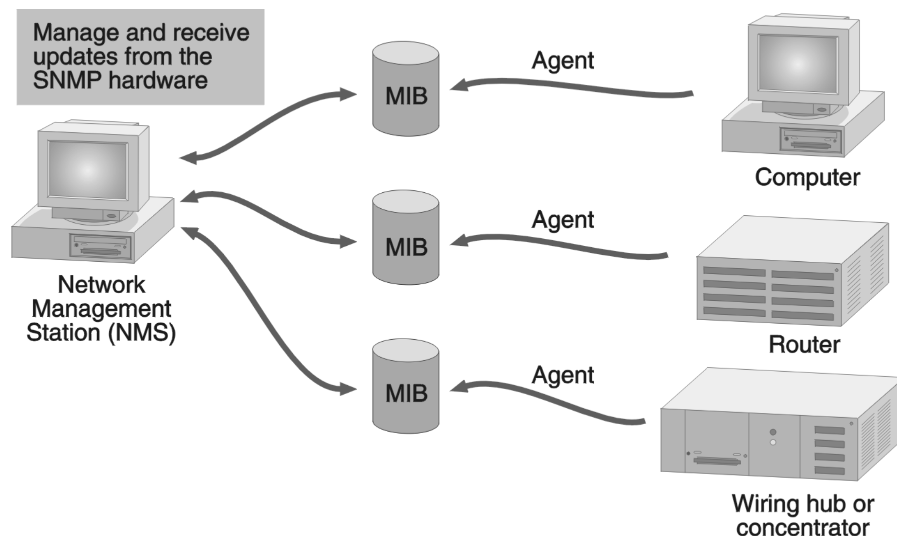
זמן לימוד משוער: 35 דקות

סקירה כללית של SNMP

SNMP הוא תקן ניהול רשת הנמצא בשימוש נרחב ברשתות TCP/IP, ובנוסף, לאחרונה, ברשתות IPX (**I**nternet **P**acket E**x**change). SNMP מספק שיטה לניהול צמתי רשת (שרתים, תחנות עבודה, נתבים, גשרים ורכזות) מ-NMS הנמצאת במיקום מרכזי.

לביצוע שירותי הניהול, משתמש SNMP במבנה מבוזר של מערכות ניהול וסוכנים, כמתואר בתרשים 13.5. המארח הנמצא במיקום מרכזי, המפעיל תוכנת ניהול רשת, נקרא NMS, או מנהל SNMP (SNMP Manager). צמתי רשת מנוהלים מכונים סוכני SNMP.

הסוכן מדווח על מצב חומרה ומידע הגדרות תצורה למסד נתונים הנקרא MIB (**M**anagement **I**nformation **B**ase, בסיס נתונים של מידע ניהולי). MIB מגדיר את מידע החומרה והתוכנה במארח, אותו צריך סוכן SNMP לאסוף. סוכן SNMP מתקשר עם NMS כדי לספק פונקציות לבקרת התקנים.



תרשים 13.5 מבנה מבוזר המשמש את SNMP.

ניהול רשת הוא קריטי לניהול משאבים וביקורת. ניתן להשתמש ב-SNMP במספר דרכים:

- **להגדרת התקנים מרוחקים** – ניתן להגדיר מידע כך, שהוא יישלח לכל מארח רשת מה- NMS.
- **לבקרה על ביצועי רשת** – ניתן לעקוב אחר מהירות העיבוד וקיבולת הרשת, ולאסוף מידע אודות הצלחת העברות נתונים.
- **לגילוי תקלות ברשת או גישה לא מורשית** – ניתן להגדיר התרעות בהתקני רשת המתריעות על התרחשות אירועים מסוימים. כאשר מופעלת התרעה, ההתקן מעביר הודעת אירוע דרך **מנת לכידה** (Trap) אל NMS. להלן סוגים נפוצים של אירועים שעבורם ניתן להגדיר התרעה:
  - כיבוי או הפעלה מחדש של התקן.
  - גילוי כשל בקישור בנתב.
  - גישה בלתי מורשית למצב רשת.
- **לביקורת על שימוש ברשת** – ניתן לבקר את השימוש הכולל ברשת לזיהוי גישת משתמש, או קבוצה או סוגים של שימוש, עבור התקני רשת או שירותים. מידע זה יכול לשמש ליצירת חיוב ישיר של חשבונות בודדים, או של קבוצות, או להצדקת עלויות רשת בפועל או הוצאות מתוכננות.

יישום Windows 2000 של סוכן SNMP הוא שירות 32 סיביות התומך במחשבים המפעילים פרוטוקולים TCP/IP ו-IPX. Windows 2000 מיישמת גרסאות 1 ו- 2C של SNMP. גרסאות אלו מבוססות על תקנים בענף המגדירים את המבנה ואופן האחסון של מידע ניהול רשת, ואת התקשורת בין סוכנים ומערכות ניהול עבור רשתות המבוססות על TCP/IP.

לשימוש במידע המסופק על ידי שירות SNMP של Windows 2000, חייב להיות לפחות NMS אחד. שירות SNMP של Windows 2000 מספק רק את סוכן SNMP, הוא אינו כולל תוכנת ניהול SNMP. ניתן להשתמש ביישום תוכנת ניהול SNMP מגורם שלישי על המארח שיפעל כמערכת הניהול.

הערה יצרני תוכנה אחדים מתכננים מערכות ניהול רשת הפועלות על מערכות הפעלה UNIX **או** Windows NT/2000.

מערכות ניהול וסוכנים

NMS אינו חייב לפעול על אותו מחשב כמו סוכני SNMP. NMS יכול לבקש את המידע הבא מסוכני SNMP:

- זיהוי וסטטיסטיקת פרוטוקול רשת.
- זיהוי דינמי של התקנים המחוברים לרשת (הליך המכונה **גילוי**, Discovery).
- נתוני תצורת חומרה ותוכנה.
- ביצועי התקן וסטטיסטיקת שימוש.
- הודעות שגיאה ואירועים של התקן.
- סטטיסטיקת שימוש בתוכניות ויישומים.

מערכת הניהול יכולה גם לשלוח בקשה להגדרת תצורה אל הסוכן. הבקשה היא שהסוכן ישנה פרמטר מקומי, אולם זה אירוע נדיר, כיון שמרבית הפרמטרים של הלקוח הם בעלי גישה לקריאה-בלבד.

סוכני SNMP מספקים למנהלי SNMP מידע אודות פעילויות המתרחשות בשכבת פרוטוקול אינטרנט (IP) של הרשת ומגיבים לבקשות מערכת הניהול למידע. מחשב כלשהו המפעיל תוכנת סוכן SNMP, כגון שירות SNMP של Windows 2000, הוא סוכן SNMP. ניתן להגדיר את שירות הסוכן כך שיקבע איזו סטטיסטיקה יש לאגור ואילו מערכות ניהול מורשות לבקש מידע.

באופן כללי, סוכנים אינם יוזמים הודעות, הם רק מגיבים להודעות. יוצאת הדופן לכלל זה היא התרעה המופעלת על ידי אירוע מסוים. הודעת התרעה מכונה **הודעת לכידה** (Trap message). **לכידה** (Trap) היא אירוע המפעיל התרעה במחשב סוכן, כמו למשל אתחול מחדש של המערכת, או גישה בלתי מורשית. Traps ו- Trap messages מספקות אמצעי אבטחה בסיסי, על ידי הודעה למערכת הניהול על כל התרחשות של אירוע מסוג זה.

MIB - Management Information Base

מסד נתוני ניהול (**M**anagement **I**nformation **B**ase - MIB) הוא מכולת אובייקטים, שכל אחד מהם מייצג סוג מסוים של מידע. אוסף זה של אובייקטים מכיל מידע הדרוש למערכת הניהול. לדוגמה, אובייקט MIB אחד יכול לייצג את מספר ההתקשרויות (Sessions) הפעילות בסוכן, אחר יכול לייצג את כמות המקום הפנוי בדיסק הקשיח של הסוכן. כל המידע שמערכת הניהול עשויה לבקש מסוכן, מאוחסן ב-MIB שונים.

MIB מגדיר את הערכים הבאים, עבור כל אובייקט שהוא מכיל:

- ❖ שם ומזהה.
- ❖ סוג נתונים מוגדר.
- ❖ תיאור טקסט של האובייקט.
- ❖ שיטת אינדקס, המשמשת עבור אובייקטים מסוג נתונים מורכבים (המתוארים בדרך כלל כמערך רב מימדי או כנתונים בטבלה). נתונים מורכבים מתייחסים לפריטים כגון רשימת ממשקי הרשת המוגדרת במערכת, טבלת הניתוב, או טבלת ARP (**A**ddress **R**esolution **P**rotocol).
- ❖ הרשאות קריאה/כתיבה.

לכל אובייקט MIB יש מזהה ייחודי, המכיל את המידע הבא:

- ❖ סוג (מונה, מחרוזת, מדיד (gauge), או כתובת).
- ❖ רמת גישה (קריאה, או קריאה/כתיבה).
- ❖ הגבלת גודל.
- ❖ מידע טווח.

שירות SNMP של Windows 2000 תומך ב- Internet MIB II, LAN Manager MIB II, Host Resources MIB, ו-MIB של Microsoft, כגון WINS, DHCP, ו-IIS.

הודעות SNMP

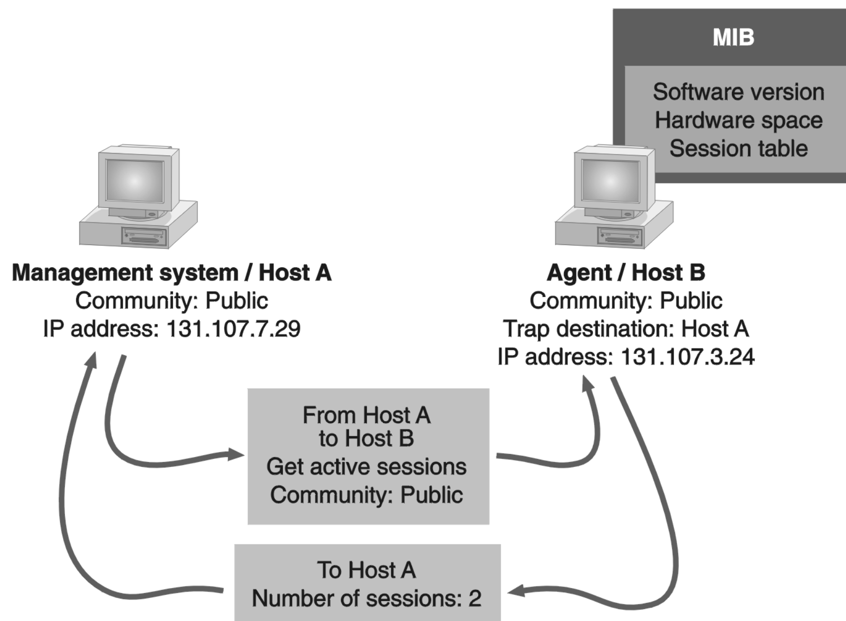
הן הסוכנים והן מערכות הניהול משתמשים בהודעות SNMP לבדיקה ותקשורת מידע אודות אובייקטים מנוהלים. הודעות SNMP נשלחות באמצעות פרוטוקול UDP (**U**ser **D**ata **P**rotocol). IP משמש לניתוב הודעות בין מערכת הניהול למארח. כברירת מחדל, יציאה 161 של UDP משמשת להאזנה להודעות SNMP, ויציאה 162 משמשת להאזנה לנתוני לכידה של SNMP.

כאשר NMS שולח בקשות להתקן רשת, תוכנית הסוכן בהתקן מקבלת את הבקשות ומאחזרת את המידע הדרוש מ-MIB. הסוכן שולח את המידע המבוקש בחזרה אל NMS שיזם את הבקשה. סוכן SNMP שולח מידע, כאשר מתרחש אירוע לכידה, או כאשר הוא מגיב לבקשת מידע ממערכת ניהול.

תוכניות מערכת הניהול והסוכן משתמשות בסוגי ההודעות הבאים:

- **GET** – הודעת הבקשה הבסיסית של SNMP. כאשר היא נשלחת על ידי NMS, היא מבקשת מידע אודות רישום MIB יחיד בסוכן - כמו למשל, כמות המקום הפנוי בדיסק.
- **GET-NEXT** – סוג מורחב של הודעת בקשה, שבה ניתן להשתמש לעיון בהיררכיה השלמה של אובייקטים מנוהלים. כאשר סוכן מעבד בקשת GET-NEXT עבור אובייקט מסוים, הסוכן מחזיר את המזהה והערך של האובייקט הבא לוגית, שלאחר המידע הקודם שנשלח. בקשת GET-NEXT שימושית בעיקר עבור טבלאות דינמיות, כגון טבלת ניתוב IP פנימית.
- **SET** – הודעה שבה ניתן להשתמש לשליחה והקצאה של ערך MIB מעודכן לסוכן, כאשר קיימת הרשאת כתיבה.
- **GET-BULK** – בקשה שהנתונים המועברים על ידי הסוכן יהיו גדולים ככל שניתן במסגרת המגבלות של גודל הודעה. הדבר מפחית את מספר העברות הפרוטוקול הנדרשות לאחזור כמות גדולה של נתוני ניהול.
- **NOTIFY** – הודעה שלא התבקשה, שנשלחת על ידי סוכן למערכת ניהול, כאשר הסוכן מזהה סוג אירוע מסוים. הודעה זו נקראת גם הודעת לכידה. לדוגמה, הודעת לכידה יכולה להישלח, כאשר מתרחש אירוע אתחול מחדש של המערכת. NMS שמקבל הודעת לכידה מכונה יעד הלכידה.

תרשים 13.6 הוא דוגמה של אופן תקשור המידע בין מערכות ניהול לסוכנים.



תרשים 13.6 אינטראקציה בין מנהל וסוכן SNMP.

הליך התקשורת הוא כדלקמן:

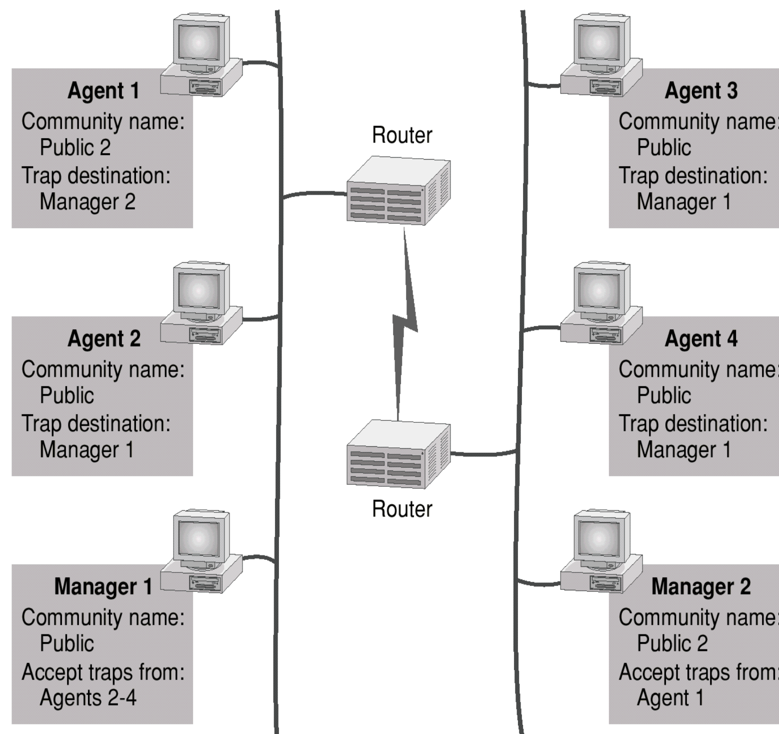
1. מערכת ניהול יוצרת הודעת SNMP, המכילה בקשת מידע (GET), שם הקהילה (Community) שאליה שייכת מערכת הניהול ויעד ההודעה - כתובת IP של הסוכן (131.107.3.24).
2. הודעת SNMP נשלחת אל הסוכן.
3. הסוכן מקבל את המנה ומפענח אותה. שם הקהילה (כברירת מחדל - Public) מאומת ומתקבל.
4. שירות SNMP קורא לסוכן המשנה המתאים לאחזור מידע ההתקשרות (Sessoin) המבוקש מ-MIB.
5. SNMP לוקח את מידע ההתקשרות מסוכן המשנה, ויוצר הודעת SNMP חוזרת, המכילה את מספר ההתקשרויות הפעילות ואת היעד - כתובת IP של מערכת הניהול (131.107.7.29).
6. הודעת SNMP נשלחת למערכת הניהול.

SNMP Communities

ניתן להקצות קבוצות מארחים לקהילות SNMP (SNMP Communities) לבדיקת אבטחה מוגבלת של סוכנים ומערכות ניהול או לצרכי מנהלה. קהילות מזוהות על ידי שמות קהילה שאתה מקצה. מארח יכול להיות שייך למספר קהילות בו-זמנית, אולם סוכן אינו מקבל בקשה ממערכת ניהול שאינה ברשימת שמות הקהילה המקובלים (Acceptable Community Names) שלו.

ניתן להגדיר קהילות באופן לוגי, או לנצל את שירות האימות הבסיסי המסופק על ידי SNMP. תרשים 13.7 מציג דוגמה של שתי קהילות, Public ו-Public 2:

- ❖ Agent 1 יכול לשלוח הודעת לכידה והודעות אחרות ל-Manager 2 כיון שהם חברים שניהם בקהילה Public 2.
- ❖ Agent 2, Agent 3 ו- Agent 4 יכולים לשלוח הודעת לכידה והודעות אחרות ל-Manager 1 כיון שכולם חברים, כברירת מחדל, בקהילה Public.



תרשים 13.7 דוגמה לשתי קהילות: Public ו- Public 2.

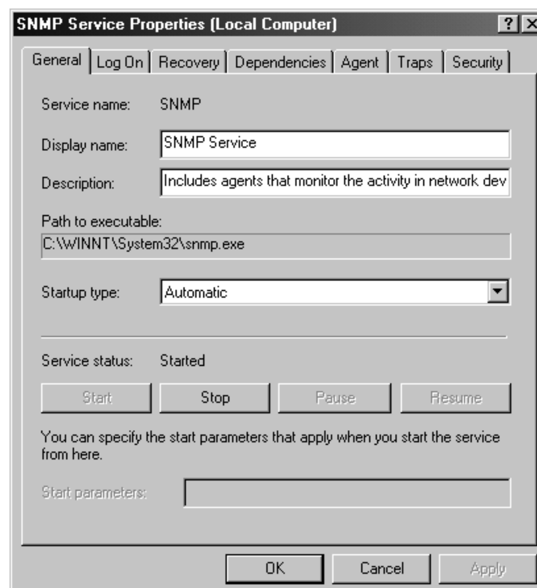
שמות קהילה מנוהלים על ידי הגדרת מאפייני אבטחת SNMP, המתוארים בהמשך שיעור זה.

הערה אין קשר כלשהו בין שמות הקהילות לבין שמות תחומים או קבוצות עבודה. שמות קהילה מייצגים סיסמה משותפת עבור קבוצות של מארחי רשת, ויש לבחור אותם ולשנות אותם, כפי שמשנים סיסמה כלשהי. ההחלטה איזה מארחים שייכים לקהילה מסוימת נקבעת בדרך כלל לפי קירבה פיסית.

התקנה והגדרה של שירות SNMP

סוכן SNMP אינו מותקן כברירת מחדל על Windows 2000 Server. הוא מותקן מהיישומון Add/Remove Programs שבלוח הבקרה. מחלון Add/Remove Programs, בחר Add/Remove Windows Components, ומאשף Windows Components המוצג, בחר Management And Monitoring Tools. הפריט Management And Monitoring Tools מכיל את Simple Network Management Protocol, שהוא סוכן SNMP. סוכן זה רשום כשירות SNMP (SNMP Service) לאחר התקנתו.

לאחר התקנת שירות SNMP, ניתן להגדיר את שירותי SNMP באמצעות הצומת Services בתוסף התוכנה Computer Management, או באמצעות תוסף התוכנה Services בקבוצת התוכניות Administrative Tools. בצומת Services, בחר SNMP Service מחלונית הפרטים, ואז בחר Properties מהתפריט Action. תוצג תיבת הדו-שיח SNMP Service Properties, כמתואר בתרשים 13.8.



תרשים 13.8 תיבת הדו-שיח SNMP Service Properties.

הערה גם SNMP Trap Service מותקן עם התקנת SNMP. שירות הלכידה מעביר מנות לכידה ממחשב מקומי או מרוחק אל יעד לכידה, בדרך כלל NMS, הפועל על המחשב המקומי.

מאפייני שירות SNMP

ניתן להשתמש בכרטיסיות General, Log On ו-Recovery בתיבת הדו-שיח SNMP Service Properties להגדרת אופן הפעלת שירות SNMP, אופן הכניסה למערכת, ואופן ההתאוששות מסיום תוכנית בלתי שגרתי של השירות או מערכת ההפעלה. שירותים אחרים הרשומים בתוסף התוכנה Computer Management מכילים את ארבע כרטיסיות אלו להגדרת שירות. הכרטיסיה General מאפשרת להפעיל או להפסיק את השירות. ניתן גם לציין שם תצוגה, תיאור, סוג אתחול ופרמטרים לאתחול. כרטיסיה אחרת, Dependencies, מספקת רשימה של השירותים (אם קיימים), התלויים בשירות SNMP, ושל השירותים שבהם SNMP תלוי. כברירת מחדל, שירות SNMP תלוי ביומן האירועים (Event Log).

מאפייני Windows 2000 SNMP Agent

סוכן SNMP מספק למערכת הניהול הקשורה את המידע אודות פעילויות המתרחשות בשכבת IP של הרשת. שירות SNMP שולח מידע סוכן בתגובה לבקשת SNMP או בהודעת לכידת SNMP.

ניתן להגדיר את מאפייני הסוכן בכרטיסיה Agent שבתיבת הדו-שיח SNMP Service Properties. הכרטיסיה Agent מכילה רשימה של השירותים בהם ניתן לבחור. שירותים אלה מתוארים בטבלה הבאה.

שירות סוכן	תנאים לבחירת שירות זה
Physical	המחשב מנהל התקנים פיסיים, כמו למשל, מחיצת דיסק קשיח.
Applications	המחשב משתמש ביישומים כלשהם, השולחים נתונים דרך TCP/IP. שירות זה צריך להיות מופעל תמיד.
Datalink and subnetwork	המחשב מנהל גשר.
Internet	המחשב הוא שער IP (נתב).
End-to-end	המחשב הוא מארח IP. שירות זה צריך להיות מופעל תמיד.

הכרטיסיה Agent גם מאפשרת להגדיר את שם האדם איתו יש ליצור קשר, כמו למשל, מנהל הרשת, ואת מיקום אדם זה. NMS עשוי להזדקק למידע זה בעת התקשרות עם סוכן SNMP.

מאפייני מנות לכידה (Trap)

מנות לכידה של SNMP יכולות לשמש במידה מוגבלת לבדיקות אבטחה. כאשר הן מוגדרות עבור סוכן, שירות SNMP מייצר הודעות לכידה בכל פעם שמתרחשים אירועים מסוימים. הודעות אלו נשלחות ליעד לכידה, בדרך כלל NMS. לדוגמה, סוכן יכול להיות מוגדר ליזום לכידת אימות, אם נשלחת בקשה למידע מצד מערכת ניהול בלתי מוכרת. ניתן גם ליצור הודעות לכידה עבור אירועים, כגון אתחול או כיבוי מערכת המארח.

ניתן להגדיר יעדי לכידה בכרטיסיה Traps שבתיבת הדו-שיח SNMP Service Properties. יעדי לכידה כוללים את שם המחשב, או כתובת IP או IPX של מערכת הניהול. יעדי לכידה חייבים להיות מארח המחובר לרשת והמפעיל תוכנת ניהול SNMP. יעדי לכידה ניתנים להגדרה על ידי משתמש, אולם האירועים (כגון אתחול המערכת) המפעילים הודעת לכידה מוגדרים באופן פנימי על ידי סוכן SNMP.

מאפייני אבטחה

ניתן להגדיר אבטחת SNMP בכרטיסיה Security של תיבת הדו-שיח SNMP Service Properties. הרשימה הבאה מתארת את האפשרויות הניתנות להגדרה בכרטיסיה Security.

- **Send authentication traps** – כאשר סוכן SNMP מקבל בקשה שאינה מכילה שם קהילה תקף, או שהמארח השולח את ההודעה אינו ברשימת המארחים המקובלים (Acceptable Hosts), הסוכן יכול לשלוח הודעה של לכידת אימות ליעד לכידה אחד או יותר (מערכות ניהול). הודעת לכידה מציינת שבקשת SNMP כשלה באימות. זוהי הגדרת ברירת המחדל.
- **Accepted community names** – כברירת מחדל, דורש שירות SNMP הגדרה של לפחות שם קהילה אחד. בדרך כלל, משמש השם Public כשם הקהילה, כיון שהוא מקובל באופן אוניברסלי בכל יישומי SNMP. ניתן למחוק או לשנות את שם ברירת המחדל, או להוסיף מספר שמות קהילה. שם הקהילה Public SNMP אינו בטוח, כיון שהשימוש בו נפוץ. לכן, כדאי לשקול הסרת שם זה. אם סוכן SNMP מקבל בקשה מקהילה שאינה ברשימה זו, הוא מייצר הודעת לכידה אימות. אם לא מוגדרים כלל שמות קהילה, סוכן SNMP דוחה את כל בקשות SNMP הנכנסות.
- **Community Rights** – ניתן לבחור רמות הרשאות המגדירות כיצד סוכן מעבד בקשות SNMP מהקהילות השונות. לדוגמה, ניתן להגדיר את רמת ההרשאות כך שתחסום את סוכן SNMP מעיבוד בקשה כלשהי מקהילה מסוימת.

- **Accept SNMP packets from any host** – בהקשר זה, מארח המקור ורשימת מארחים מקובלים מתייחסים למערכת ניהול SNMP המקורית, ולרשימת מערכות הניהול המקובלות האחרות. כאשר אפשרות זו מופעלת, אף מנת SNMP אינה נדחית על סמך שם או כתובת מקור המארח, או על סמך רשימת המארחים המקובלים. אפשרות זו מופעלת כברירת מחדל.
- **Only accept SNMP packets from these hosts** – אפשרות זו מספקת אבטחה מוגבלת. כאשר אפשרות זו מופעלת, מתקבלות רק מנות SNMP מהמארחים שברשימת המארחים המקובלים. סוכן SNMP דוחה הודעות ממארחים אחרים ושולח מנות לכידה לאימות. הגבלת הגישה למארחים הרשומים ברשימה בלבד מספקת רמת אבטחה גבוהה יותר מאשר הגבלת הגישה לקהילות מסוימות, כיון ששם קהילה יכול לכלול קבוצה גדולה של מארחים.

איתור תקלות SNMP

סעיף זה מציג שיטות לקביעת הגורם לבעיות תקשורת המיוחסות ל- SNMP. יש להפעיל עומסי פעולה רגילים בעת הבדיקות כדי לקבל משוב מציאותי.

Event Viewer

טיפול בשגיאות SNMP השתפר מאוד ב-Windows 2000. הגדרה ידנית של מאפייני רישום שגיאות SNMP הוחלף בטיפול משופר בשגיאות המשולב עם צופה האירועים. השתמש בצופה האירועים, אם מתעורר חשד לבעיה בשירות SNMP.

WINS Service

כאשר מציגים שאילתות MIBs של שרת WINS, יתכן שיהיה צורך להגדיל את פסק הזמן (Time-Out) של SNMP במערכת ההפעלה של SNMP. אם שאילתות WINS אחדות מצליחות ולאחרות אוזל הזמן, הגדל את פרק הזמן להמתנה.

כתובות IPX

אם מזינים כתובת IPX כיעד לכידה בעת התקנת שירות SNMP, יתכן שתתקבל הודעת שגיאה Error 3, כאשר מפעילים מחדש את המחשב. הדבר מתרחש כאשר מזינים כתובות IPX בצורה שגויה - על ידי שימוש בפסיק או מקף להפרדה בין מספר הרשת לכתובת MAC (**M**edia **A**ccess **C**ontrol**)**. לדוגמה, תוכנת ניהול SNMP כלשהי עשויה לקבל כתובת כגון 00008022,0002C0-F7AABD. אולם, שירות SNMP של Windows 2000 אינו מכיר בכתובת עם פסיק או מקף בין מספר הרשת לכתובת MAC.

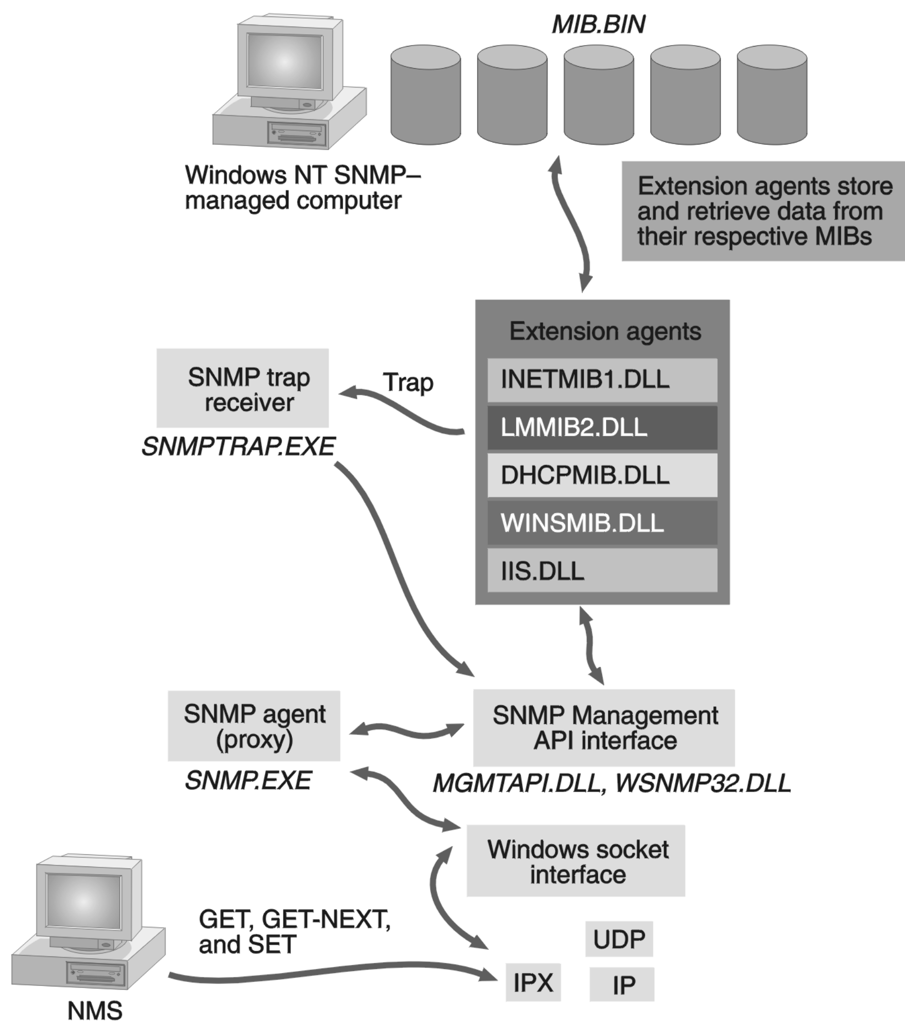
הכתובת המשמשת עבור יעד לכידה IPX חייבת להיות תואמת לתבנית 8.12 שהוגדרה על ידי IETF עבור מספר הרשת וכתובת MAC: xxxxxxxx.yyyyyyyyyyyy היכן ש-xxxxxxxx הוא מספר הרשת, ו- yyyyyyyyyyyy הוא כתובת MAC.

קבצי שירות SNMP

למען הנוחות ולסיוע באיתור תקלות, הטבלה הבאה מכילה רשימה של הקבצים הקשורים ל- SNMP, המסופקים כחלק משירות SNMP של Windows 2000.

קובץ	תיאור
Wsnmp32.dll, Mgmtapi.dll	API של מנהל SNMP המבוסס על Windows 2000. API אלה מקשיבים לבקשות מנהל, שולחים את הבקשות לסוכני SNMP ומקבלים מהם את התגובות.
*.dll	DLL של סוכני הרחבה, כגון Inetmib1.dll עבור IIS ו-Dhcpmib.dll עבור DHCP. סוכני הרחבה אלה תומכים ב-MIBs המתאימים עבור מוצרים אלה.
Mib.bin	מותקן עם שירות SNMP ומשמש את Management API (Mgmtapi.dll). הקובץ ממפה שמות אובייקטים מבוססי-טקסט אל מזהי OIDobject מספריים.
Snmp.exe	שירות סוכן SNMP; סוכן עיקרי (Proxy). תוכנית זו מקבלת בקשות תוכנית מנהל, ומעבירה את הבקשות אל DLL סוכן משנה-ההרחבה המתאים לצורך עיבוד.
Snmptrap.exe	הליך רקע. התוכנית מקבלת מנות לכידה של SNMP מסוכן SNMP, ומעבירה אותם אל API ניהול SNMP ב-MMC הניהול. התוכנית מתחילה רק כאשר API ניהול SNMP מקבל בקשה אדמיניסטרטיבית למנות לכידה.

תרשים 13.9 מציג כיצד קבצי SNMP השונים פועלים יחד לתקשורת אל NMS וממנו.



תרשים 13.9 תקשורת אל שירות SNMP וממנו.

סיכום שיעור

SNMP הוא תקן ניהול רשת, המספק שיטה לניהול התקני רשת כגון שרתים, תחנות עבודה, נתבים, גשרים, ורכזים ממארח במיקום מרכזי. כדי לבצע את שירותי הניהול, SNMP משתמש בארכיטקטורה מבוזרת של מערכות ניהול וסוכנים. מערכת הניהול של SNMP, המוכרת גם כ-NMS, יכולה לבקש מידע ממחשבים מנוהלים (סוכני SNMP). סוכני SNMP מספקים ל-NMS מידע אודות פעילויות המתרחשות בשכבת רשת IP ומגיבים לבקשות מידע ממערכת הניהול. SNMP משתמש ב-MIB כמכולה עבור אובייקטים; כל מכולה מייצגת סוג מסוים של מידע. הן סוכנים והן NMS משתמשים בהודעות SNMP לבדיקה ולתקשורת מידע אודות אובייקטים מנוהלים. ניתן להקצות קבוצות של מארחים לקהילות SNMP לבדיקת אבטחה מוגבלת של סוכנים ו-NMS או למטרות מנהלה. קהילות מזוהות במקרים רבים על ידי שמות קהילה שאתה מקצה. להגברת האבטחה, ניתן לציין את כתובת IP או שם המארח של מערכות ניהול רשת שבהן סוכן SNMP יתקשר. ניתן להגדיר את שירות SNMP דרך צומת Services של תוסף התוכנה Computer Management, או דרך תוסף התוכנה Services בקבוצת התוכניות Administrative Tools. תיבת הדו-שיח SNMP Service Properties מאפשרת להגדיר את מאפייניו השונים של שירות SNMP.

שיעור 3:
Performance Console

Windows 2000 מספקת שתי תוכניות שירות לניטור שימוש במשאבים במחשב: תוסף התוכנה System Monitor ותוסף התוכנה Performance Logs And Alerts, שתיהן מותקנות מראש על תוכנית השירות Performance. תוסף התוכנה System Monitor מאפשר מעקב אחר שימוש במשאבים ותפוקת רשת. תוסף התוכנה Performance Logs And Alerts מאפשר לאסוף נתוני ביצועים ממחשבים מקומיים, או מרוחקים.

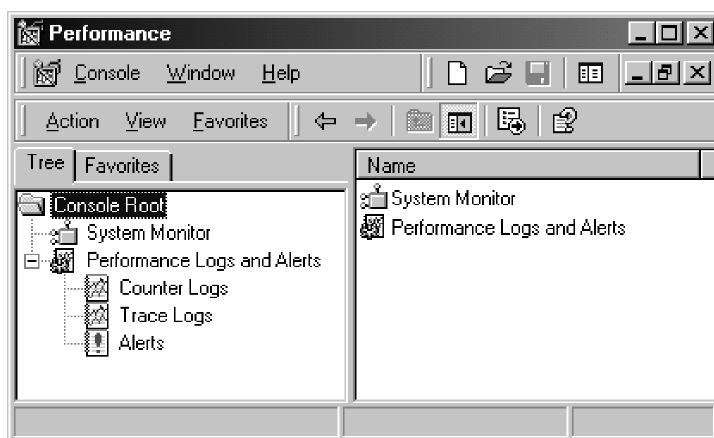
לאחר שיעור זה, תוכל

- להשתמש בתוספי התוכנה System Monitor ו-Performance Logs And Alerts הנמצאים בתוכנית השירות Performance - לניטור שימוש במשאבים במחשב.

זמן לימוד משוער: 40 דקות

מבוא לתוכנית Performance

תוכנית Performance (Performance Console) היא תוכנית שירות מובנית, אליה ניתן לגשת דרך קבוצת התוכניות Administrative Tools. תוכנית Performance היא Console MMC המכילה שני תוספי תוכנה מותקנים מראש: System Monitor ו- Performance Logs And Alerts (תרשים 13.10).



תרשים 13.10 תוסף התוכנה System Monitor **ותוסף התוכנה** Performance Logs And Alerts בחלון MMC של תוכנית Performance.

עם System Monitor, ניתן לאסוף ולהציג נתוני זמן אמת אודות זיכרון, דיסק, מעבד, רשת, ופעילויות אחרות בצורת גרף, היסטוגרמה, או דוח. באמצעות Performance Logs And Alerts, ניתן להגדיר יומנים לרישום נתוני ביצועים ולהגדיר התרעות מערכת שיודיעו כאשר ערך של מונה מסוים מעל או מתחת לסף מוגדר.

ניטור ביצועי מערכת הוא חלק חשוב בתחזוקה וניהול התקנת Windows 2000 Server. ניתן להשתמש בנתוני ביצועים לצרכים הבאים:

- הבנת עומס העבודה והשפעתו על משאבי המערכת.
- זיהוי שינויים ומגמות בעומסי עבודה ושימוש במשאבים לצורך תכנון שדרוגים עתידיים.
- בדיקת שינויי הגדרות או מאמצי כוונון אחרים, על ידי ניטור התוצאות.
- אבחון בעיות ורכיבי או תהליכי יעד למיטוב.

תוסף התוכנה System Monitor ותוסף התוכנה Performance Logs And Alerts מספקים מידע מפורט אודות המשאבים המשמשים רכיבים מסוימים של מערכת ההפעלה ותוכניות שרת, אשר תוכננו לאסוף נתוני ביצועים. הגרפים מספקים תצוגה עבור נתוני ניטור-ביצועים; יומנים מספקים יכולות רישום עבור הנתונים; ואתרעות שולחות הודעות למשתמשים באמצעות שירות Messenger כאשר ערך מונה מגיע, עובר מעל או יורד מתחת לערך סף מוגדר.

התמיכה הטכנית של Microsoft משתמשת במקרים רבים בתוצאות ניטור ביצועים לאבחון בעיות. לכן, ממליצה Microsoft לנטר ביצועי מערכת כחלק משגרת הניהול.

תוסף התוכנה System Monitor

ב- Windows 2000, Performance Monitor הוחלף על ידי System Monitor. בעזרת System Monitor ניתן למדוד את הביצועים של המחשב המקומי, או של מחשבים אחרים ברשת. System Monitor מאפשר ביצוע הפעולות הבאות:

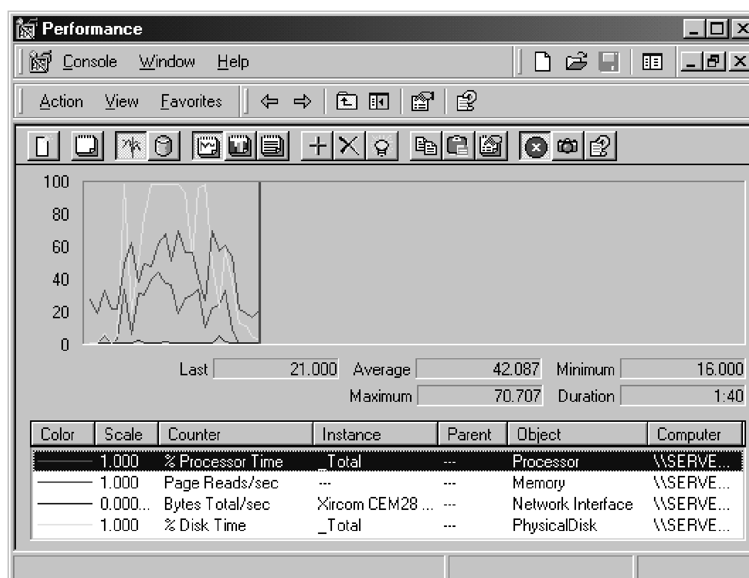
- איסוף והצגת נתוני ביצועים בזמן אמת על מחשב מקומי או ממחשבים מרוחקים.
- הצגת נתונים שנאספו כעת או שנאספו בעבר ביומן מונה (Counter).
- הצגת נתונים בתצוגת גרף, היסטוגרמה, או דוח, הניתנים להדפסה.
- שילוב פונקציונליות System Monitor לתוך Microsoft Word, או יישומים אחרים בערכת Microsoft Office באמצעות **Automation** (אוטומציה).
- יצירת דפי HTML מתצוגות ביצועים.
- יצירת תצורות ניטור לשימוש חוזר, אותן ניתן להתקין על מחשבים אחרים המשתמשים ב-MMC.

בעזרת System Monitor, ניתן לאסוף ולהציג נתונים נרחבים אודות השימוש במשאבי חומרה והפעילות של שירותי מערכת על מחשבים שאתה מנהל. ניתן להגדיר את הנתונים שרוצים לאסוף לגרף בדרכים הבאות:

- **סוג נתונים** – לבחירת הנתונים שייאספו, ניתן לציין Counter אחד או יותר של אובייקטי ניטור ביצועים. חלק מהאובייקטים (כמו למשל האובייקט זיכרון) מספקים מונים למשאבי המערכת; אחרים מספקים מונים לפעולת יישומים (לדוגמה, שירותי מערכת או יישומי Microsoft BackOffice).
- **מקור נתונים** – System Monitor יכול לאסוף נתונים מהמחשב המקומי, או ממחשבים אחרים ברשת בהם יש לך הרשאות (כברירת מחדל, נדרשת הרשאת מנהל). בנוסף, ניתן לכלול נתוני זמן אמת או נתונים שנאספו בעבר ונשמרו ביומני מונים.
- **דגימת פרמטרים** – System Monitor תומך בדגימה ידנית, לפי-דרישה או בדגימה אוטומטית המבוססת על מרווח הזמן שנקבע. בעת הצגת נתונים רשומים, ניתן גם לבחור זמני התחלה וסיום להצגת נתונים שנאספו בתקופת זמן מסוימת.

ממשק System Monitor

כאשר פותחים את תוכנית Performance, תצוגת הגרף וסרגל הכלים מוצגים כברירת מחדל, ואזור הגרף ריק. לאחר הוספת מונים לגרף, System Monitor מתחיל לשרטט ערכי מונים באזור גרף זה (ראה תרשים 13.11). חלון Tree מוסתר בתרשים 13.11 להוספת בהירות.



תרשים 13.11 תוסף התוכנה System Monitor המשרטט ערכי מונים בתצוגת גרף.

כפי שמוצג בתרשים 13.11, קיימים שלושה אזורים עיקריים בממשק System Monitor: אזור הגרף, המקרא וסרגל הערכים.

אזור הגרף

ניתן לבחור לעדכן את הנתונים אוטומטית או לפי דרישה. לעדכון לפי דרישה, השתמש בלחצן Update Data (סמל מצלמה בסרגל הכלים) להתחלה ולסיום מרווחי האיסוף. לחץ על הלחצן Clear Display (הסמל השני משמאל בסרגל הכלים) להסרת כל הנתונים מהתצוגה. להוספת מונים (Counters) לגרף, לחץ על הלחצן Add (סמל פלוס בסרגל הכלים) ובחר את המונים מתיבת הדו-שיח Add Counters.

התנועה של פס קוצב הזמן (הקו האנכי בתרשים 13.11) לרוחב הגרף מציינת את המעבר של כל מרווח עדכון. ללא קשר למרווח העדכון, התצוגה תראה עד 100 דגימות. System Monitor דוחס נתוני יומן במידה הדרושה להצגתם בתצוגה. להצגת הנתונים הדחוסים ביומן, לחץ על הלחצן Properties (הסמל הרביעי מימין בסרגל הכלים), בחר בכרטיסיה Source, בחר קובץ יומן, ואז בחר טווח זמן קצר יותר. טווחי זמן קצרים יותר כוללים פחות נתונים, כך פוחתים הסיכויים להעלמת נקודות נתונים.

ניתן גם להגדיר את התכונות הבאות של הגרף:

- סוג תצוגה, עם אפשרויות לגרף, היסטוגרמה, או דוח.
- צבע רקע של חלונית הפרטים ושל אזור תצוגת הנתונים.
- סוג, גודל, וסגנון של הגופן המשמש להצגת טקסט בתצוגה.
- צבע, רוחב, וסגנון הקו המשמש לשרטוט נתונים.

כדי להדגיש נתונים של מונה מסוים, השתמש בתכונת ההבלטה. כדי לעשות זאת יש ללחוץ על Ctrl+H או ללחוץ על הלחצן Highlight (סמל נורה) בסרגל הכלים. כאשר מבליטים בשיטה זו, הפס או הקו המייצגים נתונים עבור המונה שנבחר משנים צבע לצבע לבן עבור מרבית צבעי הרקע (כולל צבע ברירת המחדל) או שחור עבור רקע בצבע לבן או בהיר.

הערה הגדרות מפתח ברירת מחדל עבור Microsoft Word עלולות להוות סתירה לשילוב המקשים Ctrl+H, המשמש להבלטה ב- System Monitor. ייתכן שתצטרך לשנות הגדרות אלו כדי לתמוך בהבלטה, כאשר משתמשים בפקד System Monitor, שבתיקיה %systemroot%\System32\Sysmon.ocx, ב- Microsoft Word.

מקרא

השמות והמידע המתאים עבור המונים שנבחרו מוצגים במקרא (Legend), מערכת העמודות שמתחת לגרף. המקרא מציג את המידע הבא:

- **Object** – אובייקט הוא אוסף לוגי של מונים הקשורים עם משאב או שירות הניתנים לניטור.
- **Counter** – מונה הוא פריט נתונים הקשור לאובייקט. עבור כל מונה שנבחר, מציג System Monitor ערך המתאים להיבט מסוים של הביצועים המוגדרים עבור אותו אובייקט.
- **Instance** – מופע הוא מונח המשמש להבחנה בין מופעים רבים של אותו מונה במחשב. לדוגמה, מחשב בו מותקנים שני מעבדים ואנו מעוניינים לבחון את אחוז הביצועים לכל אחד מהם. שים לב שכברירת מחדל מופעי מונה רשומים לפי שם ומספר סידורי. מספר סידורי זה מוצג לאחר שם המופע, מיוצג על ידי סולמית (#) ומספר. המספר הסידורי מקל על ניטור מספר מופעים, לדוגמה, כאשר עוקבים אחר מטלות (Threads) של הליך (Process). לכיבוי תצוגת המספר הסידורי, לחץ על הלחצן Properties, ונקה את תיבת הסימון Allow Duplicate Counter Instances.

ניתן למיין ערכים בסדר עולה או יורד לפי אובייקט, מונה, מופע או מחשב, על ידי לחיצה על שם העמודה המתאימה במקרא המונים. לדוגמה, למיון לפי מונה לחץ על Counter.

הערה להתאמת קו בגרף עם המונה שערכיו מיוצגים על ידי קו זה, לחץ לחיצה כפולה על מקום בקו הגרף. המונה ייבחר במקרא. אם קווי גרף קרובים זה לזה, נסה למצוא מקום בגרף בו הם מתרחקים מעט. אחרת, ייתכן ש- System Monitor לא יוכל לאתר את הערך בו אתה מתעניין.

סרגל ערכים

סרגל הערכים (Value Bar) ממוקם מתחת לאזור הגרף ומעל המקרא. סרגל הערכים מכיל את הערך האחרון, הממוצע, המינימום והמקסימום עבור המונה שנבחר. הערכים מחושבים על פני תקופת הזמן ומספר הדגימות המוצגות בגרף, ולא על פני הזמן שחלף מאז תחילת הניטור. ערך Duration בסרגל הערכים מציין את הזמן הכולל שחלף המוצג בגרף (על סמך מרווח העדכון).

ניטור ביצועי מערכת ורשת

פעילות רשת יכולה להשפיע לא רק על ביצועי רכיבי הרשת, אלא גם ביצועי המערכת כולה. יש לנטר משאבים אחרים יחד עם פעילות רשת, כמו למשל דיסק, זיכרון ופעילות מעבד. System Monitor מאפשר לעקוב אחר פעילויות רשת ומערכת באמצעות כלי יחיד.

יש להשתמש במונים הבאים, כחלק מתצורת הניטור הרגילה:

- Cache\Data Map Hits %
- Cache\Fast Reads/sec
- Cache\Lazy Write Pages/sec
- Logical Disk\% Disk Space
- Memory\Available Bytes
- Memory\Nonpaged Pool Allocs
- Memory\Nonpaged Pool Bytes
- Memory\paged Pool Allocs
- Memory\paged Pool Bytes
- Processor(_Total)\% Processor Time
- System\Context Switches/sec
- System\Processor Queue Length
- Processor(_Total)\Interrupts/sec

ניטור פעילות רשת בעזרת System Monitor כרוך בבחינת נתוני ביצועים בכל שכבת רשת, כמוגדר במודל שבע השכבות של **O**pen **S**ystems **I**nterconnect (OSI). System Monitor מספק אובייקטי ביצועים לאיסוף נתונים המשקפים קצבי העברה, אורכי תור מנות, ונתונים אחרים של ביצועי רשת.

הערה בגלל התקורה של כותרות פרוטוקולים, קצבי העברה בפועל עשויים להיות שונים מהקצבים הרשומים עבור הכבל או הקו שבשימוש.

הטבלה הבאה מציגה מידע אודות שכבות הרשת ואובייקטי הביצועים הקשורים.

שכבת OSI	אובייקטי ביצועים
Application	שכבת היישום - Redirector, Server, Browser, ו- Server Work Queues NBT Connection (NBT הוא קיצור של NetBT, שפירושו NetBIOS על TCP/IP; NetBIOS פירושו Network Basic Input/Output System).
Transport	שכבת ההעברה - אובייקטי פרוטוקול: TCP עבור Transmission Control Protocol; UDP עבור User Datagram Protocol; NetBEUI עבור NetBIOS, AppleTalk (מותקן על ידי פרוטוקול).
Network	שכבת הרשת - מקטע רשת (מותקן כאשר מתקינים את מנהל ההתקן Network Monitor), IP עבור Internet Protocol, NWLink IPX/SPX עבור יישום Microsoft של פרוטוקול IPX/SPX (Internetwork Packet Exchange/Sequenced Packet Exchange). אובייקטי ביצועים של NWLink מציגים רק אפסים עבור מונים המדווחים אודות פעילות מסגרת. במערכות המפעילות Windows NT 4.0, התקנת Network Monitor Agent גם מתקינה את מוני Network Segment.
Data Link, Physical	שכבת קישור הנתונים והשכבה הפיסית - ממשק רשת. מונים אלה מתוחזקים על ידי מנהל ההתקן ויכולים לדווח ערכים לא מדויקים או ערכי אפס בגלל בעיות ביישום מונים על ידי מנהל ההתקן.

בעת ניטור ביצועי הרשת, כדאי להתחיל עם רכיבים ברמה הנמוכה ביותר ולעלות מעלה. נטר את האובייקטים על פני פרקי זמן הנעים בין ימים לשבועות, ולחודש. תוך שימוש בנתונים אלה, קבע **רמת בסיס לביצועים** (Performance Baseline), רמת הביצועים הצפויה בעומסי עבודה ושימוש רגילים. רמת בסיס לביצועים מהווה נקודה, אליה ניתן להשוות ביצועים לאורך זמן לזיהוי מגמות גידול, דרישות משתנות, או התהוות צוואר בקבוק. אם ביצועי רמת הבסיס לביצועים אינם מספיקים, יש לכוונן את הרשת.

כמו עם משאבים אחרים, צור רמת בסיס לביצועים עבור ביצועי רשת. כאשר נתוני הביצועים אינם תואמים את ערכי רמת הבסיס לביצועים, חקור את הגורם. ערכי מונה רשת חריגים בשרת מציינים במקרים רבים בעיות בזיכרון, במעבד או בדיסקים של השרת. לכן, הגישה הטובה ביותר לניטור שרת היא התייחסות למוני הרשת בשילוב עם Processor\% Processor Time, PhysicalDisk\% Disk Time, ו-Memory\Pages/sec (זמן מעבד, זמן דיסק וזמן זיכרון).

לדוגמה, אם גידול דרמתי ב-Pages/sec מלווה בירידה ב-Bytes Total/sec המטופלים על ידי שרת, ככל הנראה סובל המחשב ממחסור בזיכרון פיסי לפעולות רשת. מרבית משאבי רשת, כולל מתאמי הרשת ותוכנת הפרוטוקול, משתמשים בזיכרון שלא ניתן להוריד לקובץ החלפה (Unpaged). אם מחשב מחליף (Paging) בצורה מופרזת, ייתכן שהדבר נובע מכך שרוב הזיכרון הפיסי שלו הוקצה לפעילויות רשת, ונשארה רק כמות קטנה של זיכרון עבור הליכים המשתמשים בזיכרון, שניתן להוריד לקובץ החלפה (Paged). כדי לוודא מצב זה, בדוק את יומן האירועים של המערכת וחפש רישומים המצביעים על מחסור בזיכרון Paged או Unpaged. נטר גם את המונים בקובץ החלפה (Unpaged Pool Memory) וזיכרון כולל.

אובייקטי דיסק ותוכנית השירות Diskperf

שני אובייקטי דיסק עיקריים מכילים מונים ב-System Monitor, האובייקטים PhysicalDisk ו-LogicalDisk. כברירת מחדל ב- Windows 2000 Server, מוני הביצועים של הדיסק הפיסי מופעלים ואלה של הדיסק הלוגי אינם מופעלים. מוני הביצועים של הדיסק הלוגי מופעלים באמצעות תוכנית השירות Diskperf משורת הפקודה. השתמש בפקודה **diskperf -yv** להפעלת מוני הביצועים Logical Disk.

לאחר הפעלת פקודה זו, יש לאתחל מחדש את המחשב. עם האתחול, יופעלו מוני הביצועים של הדיסק הפיסי והדיסק הלוגי. מונים אלה מוכלים באובייקטים PhysicalDisk ו-LogicalDisk של System Monitor בהתאמה.

קיימת עלות קטנה בביצועים, הנובעת מהפעלת מונים אלה. אם אינך מנטר ביצועי דיסק, הקלד **diskperf -n** לנטרול שני האובייקטים והמונים שלהם.

ניתן להפעיל או לנטרל לפי בחירה את שני מוני הביצועים הפיסי והלוגי באמצעות Diskperf.

תוסף התוכנה
Performance Logs and Alerts

בעזרת Performance Logs And Alerts, ניתן לאסוף באופן אוטומטי נתוני ביצועים ממחשבים מקומיים או מרוחקים. ניתן להציג נתוני מונה רשומים באמצעות System Monitor, או לייצא את הנתונים לתוכניות גיליון נתונים או מסדי נתונים, לניתוח ויצירת דוחות. שים לב, שמכיון שרישום היומן פועל כשירות, איסוף הנתונים יכול להתבצע ללא תלות בכניסת משתמשים כלשהם למחשב המנוטר.

תוסף התוכנה Performance Logs And Alerts מאפשר לבצע את הפעילויות הבאות:

- איסוף נתונים בתבנית מופרדת בפסיקים (csv) או מופרדת בטאבים המאפשרת ייצוא קל אל תוכניות גיליון נתונים. ניתן להשתמש גם בתבנית קובץ-יומן בינארית לרישום מעגלי או לרישום מקרים, כגון הליכים, או תהליכים שעשויים להתחיל לאחר שהיומן מתחיל לאסוף נתונים (רישום מעגלי, Circullar Logging, הוא הליך של רישום נתונים ברציפות לקובץ יחיד, תוך כתיבת נתונים חדשים על גבי נתונים ישנים).

- הצגת נתוני מונה במהלך האיסוף ולאחר סיום האיסוף.

- הגדרת זמני התחלה וסיום, שמות קבצים, גודלי קבצים, ופרמטרים אחרים ליצירת יומנים אוטומטית.

- ניהול מספר הליכים של רישום יומן מחלון Console בודד.

- הגדרת התרעה על מונה, ובכך קביעה שתישלח הודעה, תופעל תוכנית, או שיתחיל יומן, כאשר הערך במונה הנבחר עולה מעל או נופל מתחת לערך מסוים.

בדומה ל- System Monitor, Performance Logs And Alerts תומך בדברים הבאים: 1) הגדרת אובייקטי ביצועים, מוני ביצועים ומקרי אובייקט. 2) הגדרת מרווחי דגימה לניטור נתונים אודות משאבי חומרה ושירותי מערכת. Performance Logs And Alerts מציע גם פעולות נוספות, הקשורות לרישום נתוני ביצועים, והן:

- התחלה וסיום רישום יומן - ידנית לפי דרישה או אוטומטית, על סמך לוח זמנים המוגדר על ידי המשתמש.

- יצירת יומני מעקב. על ידי שימוש בספק נתוני מערכת ברירת המחדל, או בספק אחר, יומני מעקב רושמים נתונים כשמתרחשות פעילויות מסוימות, כגון פעולות קלט/פלט דיסק או שגיאות עמוד. כשמתרחש האירוע, הספק שולח את הנתונים לשירות Performance Logs And Alerts. רישום ושליחת נתונים אלה שונה מהפעילות של יומני מונה. כשמשתמשים ביומן מונה, השירות מכיל נתונים מהמערכת בתום מרווח העדכון, ולא כשמתרחש אירוע מסוים. דרוש כלי ניתוח (Parsing) לפענוח מוצא יומן המעקב. אנשי פיתוח יכולים ליצור כלי כגון זה, באמצעות ממשקי תכנות יישומים - APIs (**A**pplication **P**rogramming **I**nterfaces) המסופקים באתר האינטרנט של Microsoft, **http://msdn.microsoft.com/**.

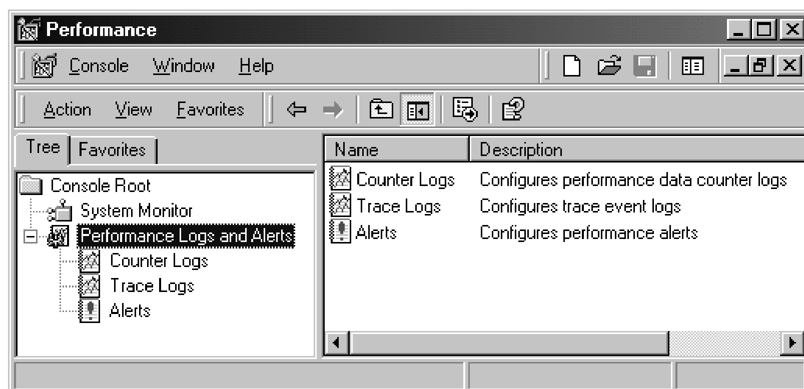
- הגדרת תוכנית שפועלת עם עצירת יומן.

- הגדרת הגדרות נוספות עבור רישום יומנים אוטומטי, כגון שינוי שמות קבצים אוטומטי, והגדרת פרמטרים לעצירה והתחלת יומן, על בסיס זמן שחלף או גודל קובץ.

הערה ניתן לעבוד עם נתונים מקובץ יומן, בזמן שהשירות אוסף נתונים וקובץ היומן נעול. לדוגמה, Microsoft Excel יכול לייבא קובץ יומן פעיל, אולם הוא יפתח עותק לקריאה בלבד של היומן הנעול.

ממשק Performance Logs And Alerts

ב- Performance Logs And Alerts, ניתן להגדיר הגדרות עבור יומני מונים, יומני מעקב והתרעות. חלונית הפרטים של תוסף התוכנה מציגה יומנים והתרעות שיצרת (תרשים 13.12).



תרשים 13.12 יומנים והתרעות בתוסף התוכנה Performance Logs And Alerts.

ניתן להגדיר מספר יומנים או התרעות שיפעלו במקביל. כל יומן או התרעה הוא הגדרת תצורה שמורה שבחרת. אם הגדרת את היומן להפעלה ועצירה אוטומטיים, יומן יחיד יכול ליצור הרבה קבצי נתונים נפרדים ביומן. לדוגמה, אם יצרת קובץ יומן עבור הפעילות של כל יום, קובץ אחד ייסגר ב- 23:59 היום, וקובץ חדש ייפתח ב - 00:00 מחר.

הטבלה שלהלן מסבירה את מידע סיכום השאילתה המסופק על ידי העמודות בחלון הפרטים.

עמודה	תיאור
Name	שם היומן או ההתרעה. ניתן לחשוב על כך כ"שם ידידותי" המתאר את סוג הנתונים הנאספים או את המצב שמנטרים. יומן אחר יכול ליצור מספר קבצי יומן. שים לב שקובץ יומן לדוגמה, בשם System Overview, הוגדר מראש עבור יומני מונים. ניתן להתחיל רישום ביומן, באמצעות קובץ זה, או על ידי הגדרת הגדרות אחרות המתאימות לצרכיך.

עמודה	תיאור
Comment	יכול לכלול מידע תיאורי כלשהו אודות היומן או ההתרעה.
Log File Type	זו תבנית קובץ היומן שהגדרת. עבור התרעה, הסוג יהיה תמיד התרעה (Alert), עבור יומני מעקב, הוא יהיה תמיד רציף (Sequential). עבור יומנים, הסוג יכול להיות בינארי, בינארי מעגלי, טקסט- CSV (עבור טקסט מופרד בפסיקים), או טקסט - TSV (עבור טקסט מופרד בטאבים).
Log File Name	זהו הנתיב ושם קובץ הבסיס המוגדר עבור קבצים המיוצרים על ידי יומן זה. שם קובץ הבסיס משמש לשינוי שמות קבצים חדשים אוטומטית.

להצגת פרמטרים המוגדרים עבור כל יומן, בחר את שם היומן בחלון הפרטים ואז בחר Properties מתפריט Action. בתיבת הדו-שיח המוצגת, ניתן לבחור כיצד לתת שם לקבצי היומן, מתי רישום יומן מתוזמן להתרחש, ואיזה אובייקטי ביצועים ומונים רוצים לנטר ביומן.

אם יומן פעיל ואוסף נתונים כעת (על סמך לוח זמנים שקבעת עבור היומן או ההתרעה), מוצג סמל נתונים ירוק לצד היומן או ההתרעה. אם מוצג סמל אדום, היומן או ההתרעה הוגדרו, אולם אינם פעילים כעת.

הערה ניתן להגדיר יותר מסוג אחד של יומן שיפעל בזמן מסוים. יומן אחד יכול ליצור מספר קבצי יומן, אם נבחרה אפשרות ההתחלה מחדש, או אם מתחילים ומפסיקים את היומן מספר פעמים. אולם, לא ניתן לראות קבצי יומן שונים אלה בחלון MMC Console. השתמש בסייר Windows להצגת רשימה של קבצים אלה.

סיכום שיעור

הכלי Performance בקבוצת התוכניות Administrative Tools מכיל שתי תוכניות שירות לניטור שימוש במשאבים במחשב: תוסף התוכנה System Monitor ותוסף התוכנה Performance Logs And Alerts. System Monitor מאפשר למדוד את הביצועים של המחשב המקומי או של מחשבים אחרים ברשת. בעזרת System Monitor, ניתן לאסוף ולהציג נתונים נרחבים אודות השימוש במשאבי חומרה והפעילות של שירותי מערכת במחשבים שאתה מנהל. קיימים שלושה אזורים עיקריים בממשק System Monitor: אזור הגרף, המקרא וסרגל הערכים. System Monitor מספק אובייקטי ביצועים לאיסוף נתונים המשקפים קצבי העברה, אורכי תור מנות ונתונים אחרים על ביצועי הרשת. כל אובייקט הוא אוסף לוגי של מונים. עבור כל מונה שנבחר, System Monitor מציג ערך המתאים להיבט מסוים של הביצועים המוגדר עבור אובייקט הביצועים. בעזרת Performance Logs And Alerts, ניתן לאסוף נתוני ביצועים אוטומטית ממחשבים מקומיים או מרוחקים. בדומה ל- System Monitor, גם Performance Logs And Alerts מאפשר להגדיר אובייקטי ביצועים, מוני ביצועים ומקרי אובייקטים, ולהגדיר מרווחי דגימה לניטור נתונים, אודות משאבי חומרה ושירותי מערכת. ב-Performance Logs And Alerts, מגדירים הגדרות עבור יומנים, יומני מעקב והתרעות. חלונית הפרטים של Performance Console מציגה יומנים והתרעות שיצרת.

שיעור 4: ניטור רשת

שלא כמו System Monitor, המשמש לניטור כל דבר מחומרה ועד תוכנה, Network Monitor (מנטר הרשת) מתמקד רק בפעילות רשת. Network Monitor מאפשר להציג פעילות רשת ולזהות בעיות ברשת. לדוגמה, ניתן להשתמש ב-Network Monitor לאבחון בעיות חומרה ותוכנה, כאשר שני מחשבים או יותר אינם יכולים לתקשר ביניהם. ניתן גם להעתיק יומן של פעילות רשת לתוך קובץ, ואז לשלוח את הקובץ למנתח רשתות מומחה או ארגון תמיכה. אנשי פיתוח יישומי רשת יכולים להשתמש ב- Network Monitor לניטור ואיתור תקלות ביישומי רשת עם פיתוחם.

לאחר שיעור זה, תוכל

- להשתמש ב- Network Monitor ללכידה והצגת מסגרות רשת.

זמן לימוד משוער: 35 דקות

סקירה כללית של Network Monitor

Network Monitor עוקב אחר תפוקת רשת במונחים של תעבורת רשת שנלכדה. Network Monitor מנטר תעבורה רק במקטע הרשת המקומי. לניטור תעבורה מרוחקת, יש להשתמש בגרסת Network Monitor המשווקת עם **S**ystems **M**anagement **S**erver (SMS) של Microsoft, גירסה 1.2 או 2.0.

Network Monitor מנטר את זרם נתוני הרשת, הכולל את כל המידע המועבר על פני הרשת בזמן נתון. לפני העברה, מחולק מידע זה על ידי תוכנת הרשת לחלקים קטנים יותר, המכונים מסגרות (Frames) או מנות (Packets). כל מסגרת מורכבת מהמידע הבא:

- כתובת המקור של המחשב ששלח את ההודעה.
- כתובת היעד של המחשב המקבל את המסגרת.
- כותרות מכל פרוטוקול המשמש לשליחת המסגרת.
- הנתונים או חלק מהנתונים הנשלחים.
- סיומת המכילה בדרך כלל CRC לוידוא שלמות המסגרת.

ההליך שבאמצעותו מעתיק Network Monitor מסגרות מכונה **לכידה** (Capturing). ניתן להשתמש ב- Network Monitor ללכידת כל תעבורת הרשת המקומית, או שניתן לבודד מערכת משנה של מסגרות ללכידה. ניתן גם לגרום ללכידה להגיב לאירועים ברשת. לדוגמה, ניתן לגרום לרשת להפעיל קובץ הפעלה כאשר Network Monitor מזהה מערכת תנאים מסוימת ברשת. הדבר דומה לתכונת התרעות המערכת בתוסף התוכנה Performance Logs And Alerts.

לאחר לכידת נתונים, ניתן להציגם בממשק המשתמש של Network Monitor. Network Monitor מבצע חלק ניכר מניתוח הנתונים עבורך, על ידי תרגום נתוני הלכידה הגולמיים למבנה המסגרות הלוגי.

לאבטחה, Network Monitor של Windows 2000 לוכד רק את אותן מסגרות, כולל מסגרות שידור רחב (Broadcast) ושידור מרובה (Multicast), הנשלחות אל או מהמחשב המקומי. Network Monitor גם מציג סטטיסטיקה כוללת של מקטע הרשת עבור מסגרות שידור, מסגרות שידור מרובה, שימוש ברשת, סך בתים שהתקבלו בשנייה וסך מסגרות שהתקבלו בשנייה.

כדי לסייע בהגנה על הרשת מפני שימוש בלתי מורשה בהתקנות Network Monitor, יכול Network Monitor לזהות התקנות אחרות של Network Monitor הפועלות על המקטע המקומי של הרשת. Network Monitor גם מזהה את כל המופעים של מנהל התקן Network Monitor בשימוש מרחוק (על ידי Network Monitor מ- Systems Management Server או אובייקט Network Segment ב- System Monitor) ללכידת נתונים ברשת.

כאשר Network Monitor מזהה התקנות אחרות של Network Monitor הפועלות ברשת, הוא מציג את המידע הבא:

- שם המחשב.
- שם המשתמש שנכנס למחשב זה.
- מצב Network Monitor על המחשב המרוחק (הפעלה, לכידה, או העברה).
- כתובת מתאם הרשת של המחשב המרוחק.
- מספר הגירסה של Network Monitor על המחשב המרוחק.

במקרים מסוימים, עלולה ארכיטקטורת הרשת למנוע מהתקנה אחת של Network Monitor לזהות התקנה אחרת. לדוגמה, אם התקנה מופרדת מזו שלך, על ידי נתב שאינו מעביר שידורים מרובים (Multicast), ההתקנה שלך לא תוכל לזהות את ההתקנה האחרת.

Network Monitor משתמש בתכונת מפרט ממשק מנהל התקן רשת (NDIS - **N**etwork **D**river **I**nterface **S**pecification), להעתקת כל המסגרות שהוא מזהה לחוצץ הלכידה, אזור אחסון בזיכרון בעל אפשרות שינוי גודל. גודל ברירת המחדל הוא 1MB, אך ניתן לשנות את הגודל ידנית, לפי הצורך. החוצץ הוא קובץ ממופה-זיכרון ותופס מקום בדיסק.

הערה **כיון ש-** Network Monitor משתמש במצב המקומי-בלבד של NDIS, במקום במצב הכללי (בו מתאם הרשת מעביר את כל המסגרות שנשלחות ברשת), ניתן להשתמש ב-Network Monitor גם אם מתאם הרשת אינו תומך במצב הכללי (Promiscuous). **ביצועי** הרישות אינם מושפעים משימוש במנהל התקן NDIS ללכידת מסגרות (העברת המתאם למצב כללי עשויה להוסיף 30 אחוזים או יותר לעומס על המעבד).

התקנת Network Monitor Tools

Network Monitor Tools כוללים את Network Monitor Console ואת מנהל ההתקן Network Monitor. כלים אלה אינם מותקנים כברירת מחדל על Windows 2000 Server. ניתן להתקין אותם מהיישומון Add/Remove Programs שבלוח הבקרה. מהחלון Add/Remove Programs, בחר את Add/Remove Windows Components ומאשף Windows Components המוצג, בחר Management And Monitoring Tools. הפריט Management And Monitoring Tools מכיל את Network Monitor Tools. לאחר ההתקנה, מוצגת Network Monitor Console בקבוצת התוכניות Administrative Tools ו-Network Monitor Driver רשום בתיבת הדו-שיח Local Area Connection Properties.

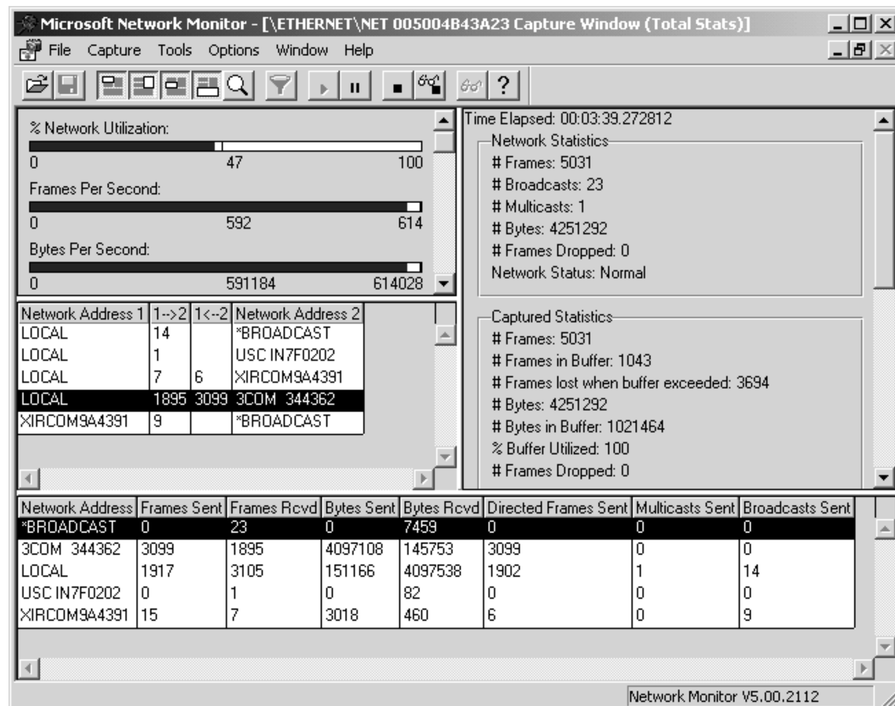
לכידת נתוני מסגרות

ללכידת נתוני מסגרות, Network Monitor ומנהל ההתקן של Network Monitor חייבים להיות מותקנים על מחשב Windows 2000. מנהל ההתקן של Network Monitor (המכונה גם סוכן Network Monitor) מאפשר ל- Network Monitor לקבל מסגרות ממתאם רשת ומאפשר ל- Network Monitor המצויד ב-SMS ללכוד ולהציג מסגרות ממחשב מרוחק, כולל אלה עם חיבור רשת בחיוג. כאשר המשתמש במחשב המפעיל SMS Network Monitor מתחבר מרחוק אל מחשב עליו הותקן מנהל התקן Network Monitor, ומשתמש זה יוזם לכידה, סטטיסטיקת רשת נלכדת באופן מקומי על המחשב המפעיל את מנהל התקן Network Monitor, והנתונים מהלכידה מוצגים באמצעות המחשב המנהל.

הערה מנהלי התקנים Network Monitor עבור מערכות הפעלה אחרות של Windows, מלבד Windows 2000, מצוידים ב-SMS. כאשר מתקינים את Network Monitor על מחשב Windows 2000, מנהל התקן Network Monitor מותקן אוטומטית.

ללכידת נתונים, פתח את Network Monitor ומהתפריט Capture בחר Start. עם לכידת מסגרות מהרשת, סטטיסטיקה אודות המסגרות תוצג בחלון Network Monitor Capture, כמתואר בתרשים 13.13.

Network Monitor מציג סטטיסטיקת קישור ממאם קישורי הרשת הייחודיים הראשונים שהוא מזהה. לאיפוס סטטיסטיקה והצגת מידע אודות 100 הקישורים הבאים המזוהים, בחר מתפריט Capture את האפשרות Clear.



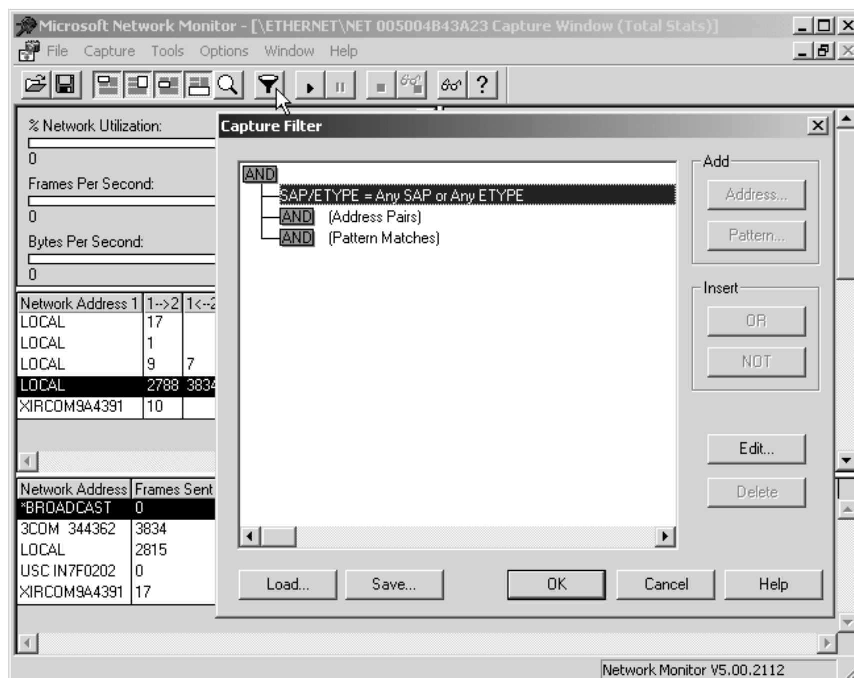
תרשים 13.13 חלון Capture של ממשק Network Monitor.

שימוש במסנני לכידה

מסנן לכידה (Capture Filter) פועל כמו שאילתה למסד נתונים. ניתן להשתמש בו לציון סוגי מידע הרשת שרוצים לנטר. לדוגמה, להצגת מערכת משנה מסוימת בלבד של מחשבים או פרוטוקולים, ניתן ליצור מסד נתוני כתובות, להשתמש במסד הנתונים להוספת כתובות למסנן, ואז לשמור את המסנן לקובץ. על ידי סינון מסגרות, ניתן לחסוך הן במשאבי החוצץ (Buffer) והן בזמן. מאוחר יותר, אם יש צורך, ניתן לטעון את קובץ מסנן הלכידה ולהשתמש במסנן שוב.

לתכנון מסנן לכידה, ציין משפטי החלטה בתיבת הדו-שיח Capture Filter (תרשים 13.14).

לפתיחת תיבת הדו-שיח Capture Filter, בחר Filter מהתפריט Capture, לחץ על סמל המשפך בסרגל הכלים (תרשים 13.14), או הקש על F8. תיבת הדו-שיח מציגה את עץ ההחלטות של המסנן, שהוא תצוגה גרפית של לוגיקת המסנן. כאשר כוללים או שוללים מידע ממפרטי הלכידה, עץ ההחלטות משקף מפרטים אלה.



תרשים 13.14 תיבת הדו-שיח Capture Filter.

סינון לפי פרוטוקול

ללכידת מסגרות המשתמשות בפרוטוקול מסוים, ציין את הפרוטוקול בשורה =SAP/ETYPE של מסנן הלכידה. לדוגמה, ללכידת מסגרות IP בלבד, נטרל את כל הפרוטוקולים ואז הפעל את ETYPE 0x800 IP ואת SAP 0x6 IP. כברירת מחדל, כל הפרוטוקולים הנתמכים על ידי Network Monitor מופעלים.

סינון לפי כתובת

ללכידת מסגרות ממחשבים מסוימים ברשת, ציין זוג אחד או יותר של כתובות במסנן לכידה. ניתן לנטר עד ארבעה זוגות כתובות מסוימים בו-זמנית.

זוג כתובות מורכב מהפריטים הבאים:

- ❖ כתובות שני המחשבים שאת התעבורה ביניהם רוצים לנטר.
- ❖ חיצים המציינים את כיוון התעבורה שרוצים לנטר.
- ❖ מילת המפתח INCLUDE או EXCLUDE (לכלול, או פרט ל...), המציינת כיצד Network Monitor יגיב למסגרת העונה על המפרט.

ללא תלות בסדר בו מוצגים משפטים בתיבת הדו-שיח Capture Filter, משפטי EXCLUDE מוערכים תחילה. לכן, אם מסגרת עונה על הקריטריונים המצוינים במשפט EXCLUDE במסנן המכיל הן משפט INCLUDE והן משפט EXCLUDE, מסגרת זו אינה נלכדת. Network Monitor אינו בודק מסגרת זו על ידי משפטי INCLUDE כדי לבדוק אם היא עונה גם על קריטריון זה.

סינון לפי תבנית נתונים

על ידי ציון התאמת תבנית נתונים במסנן לכידה, ניתן:

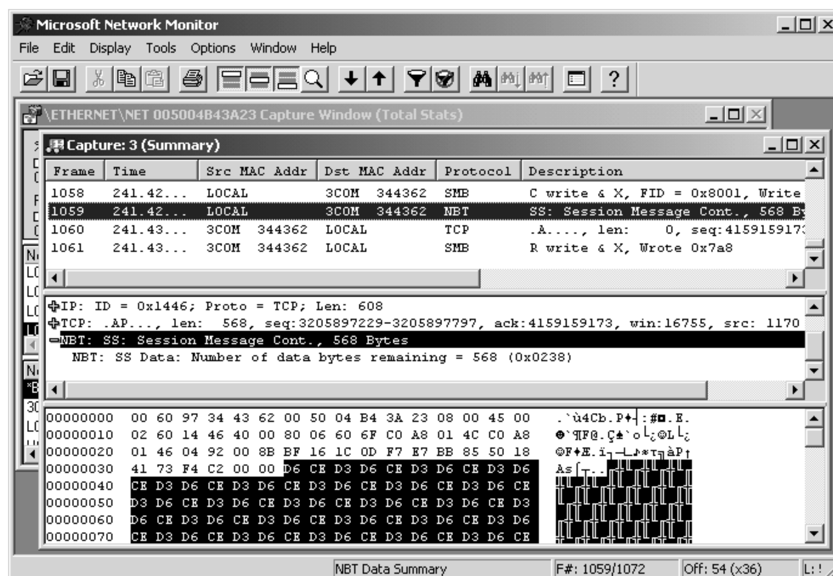
- ❖ להגביל לכידה לאותן מסגרות המכילות תבנית מסוימת של נתוני ASCII או נתונים הקסדצימליים בלבד.
- ❖ לציין כמה בתים (Offsets) לתוך המסגרת חייבת להתקיים התבנית.

כאשר מסננים על סמך התאמת תבנית בנקודה מסוימת של הנתונים, יש לציין היכן התבנית מופיעה במסגרת (כמה בתים מההתחלה או מהסוף). אם אמצעי הרשת משתמש במסגרות בעלות גודל משתנה, יש לציין להתחיל לספור פנימה עבור התאמת תבנית של כותרת הטופולוגיה.

הצגת נתונים לכודים

כדי לפשט ניתוח נתונים, Network Monitor מפענח נתונים גולמיים הנאספים בלכידה ומציג אותם בחלון Capture. להצגת מידע לכוד בחלון Capture, לחץ על Stop And View בתפריט Capture, בעת הפעלת הליך הלכידה. ניתן גם להציג את החלון Capture על ידי פתיחת קובץ בעל סיומת cap. אם עצרת לכידה, ניתן להציג את הנתונים בחלון Capture על ידי בחירה ב- Display Captured Data מהתפריט Capture, לחיצה על סמל המשקפיים בסרגל הכלים, או הקשה על F12.

תרשים 13.15 מציג את רכיבי המפתח בחלון Capture.



תרשים 13.15 חלון Capture ב- Network Monitor.

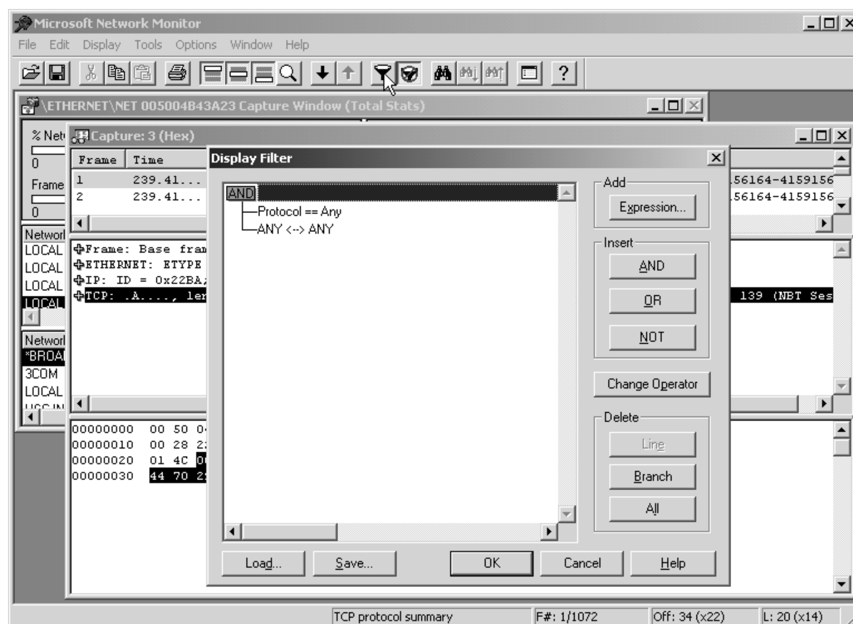
שימוש במסנני תצוגה

ניתן להשתמש במסנן תצוגה (Display Filter) לקביעה איזה מסגרות יוצגו. כמו מסנן הלכידה, גם מסנן התצוגה פועל כמו שאילתה למסד נתונים, ומאפשר לבודד סוגים מסוימים של מידע. אולם, מכיון שמסנן תצוגה פועל על נתונים שכבר נלכדו, הוא אינו משפיע על תוכן חוצץ הלכידה של Network Monitor.

ניתן לסנן מסגרת לפי המידע הבא:

- ❖ כתובת מקור או יעד המסגרת.
- ❖ הפרוטוקולים ששימשו לשליחת המסגרת.
- ❖ המאפיינים והערכים המוכלים במסגרת (מאפיין הוא שדה נתונים בתוך כותרת פרוטוקול. המאפיינים של פרוטוקול מציינים את מטרת הפרוטוקול).

כדי שתוצג תיבת הדו-שיח Display Filter חייב חלון הלכידה להיות במוקד Network Monitor. תרשים 13.16 מציג את תיבת הדו-שיח Display Filter, שהגישה אליה דרך התפריט Display, על ידי הקשה על F8, או על ידי לחיצה על סמל המשפך בסרגל הכלים.



תרשים 13.16 תיבת הדו-שיח Display Filter.

כדי לתכנן מסנן תצוגה, ציין משפטי החלטה בתיבת הדו-שיח Display Filter. מידע בתיבת הדו-שיח Display Filter מוצג בצורת עץ החלטות, שהוא תצוגה גרפית של לוגיקת המסנן. כאשר משנים מפרטי מסנן תצוגה, עץ ההחלטות משקף שינויים אלה. יש ללחוץ על OK לשמירת משפט ההחלטה הרצוי והוספתו לעץ ההחלטות לפני הוספת משפט החלטה נוסף.

למרות שמסנני לכידה מוגבלים לארבעה ביטויי סינון כתובות, מסנני תצוגה אינם מוגבלים. עם מסנני תצוגה, ניתן גם להשתמש בלוגיקת AND, OR ו-NOT. כאשר מציגים נתונים לכודים, כל המידע הזמין אודות המסגרות הלכודות מוצג בחלון Frame Viewer. להצגת רק אותן מסגרות שנשלחו על ידי פרוטוקול מסוים, ערוך את השורה Protocol בתיבת הדו-שיח Display Filter.

מאפייני פרוטוקול הם מידע המגדיר את מטרת הפרוטוקול. כיון שמטרת פרוטוקולים משתנה, מאפיינים יהיו שונים זה מזה בפרוטוקולים שונים. נניח, למשל, שלכדת מספר גדול של מסגרות המשתמשות בפרוטוקול SMB, אולם ברצונך להתבונן רק באותן מסגרות שבהן פרוטוקול SMB שימש ליצירת ספריה במחשב שלך. במקרה זה, ניתן לבודד מסגרות שבהן מאפיין פקודת SMB שווה לפקודה Make Directory.

כאשר מציגים נתונים לכודים, כל הכתובות מהן נלכד המידע מוצגות בחלון Frame Viewer. להצגת רק אותן מסגרות שמקורן במחשב מסוים, ערוך את השורה ANY < - > ANY בתיבת הדו-שיח Display Filter.

נושאי ביצועים ב- Network Monitor

Network Monitor יוצר קובץ ממופה-זיכרון עבור חוצץ הלכידה (Capture Buffer) שלו. לקבלת התוצאות הטובות ביותר, יש לוודא יצירת חוצץ לכידה גדול מספיק לאחסון התעבורה הרצויה.

בנוסף, למרות שלא ניתן לשנות את גודל המסגרת, ניתן לאחסן רק חלק מהמסגרת, ובכך להפחית את כמות המקום המבוזבז בחוצץ הלכידה. לדוגמה, אם מעוניינים רק בנתונים בכותרת המסגרת, ניתן להגדיר את גודל המסגרת (בבתים) לגודל כותרת המסגרת. Network Monitor משליך את נתוני המסגרת בעת אחסון המסגרות בחוצץ הלכידה, וכך נעשה שימוש בפחות מקום בחוצץ הלכידה.

הפעלת Network Monitor ברקע היא דרך אפשרית להפחתת כמות משאבי הרשת הדרושים להפעלת התוכנית. כדי להפעיל את Network Monitor ברקע, בחר Dedicated Capture Mode בתפריט Capture. זוהי אחת השיטות להפחתת שימוש במשאבים, אם מנות הרשת נופלות במקום להילכד.

סיכום שיעור

Network Monitor מאפשר להציג ולזהות בעיות ברשתות. הוא עוקב אחר תפוקת רשת במונחים של תעבורת רשת לכודה. Network Monitor מנטר את זרם הנתונים במקטע המקומי, הכולל את כל המידע המועבר במקטע הרשת בזמן נתון כלשהו. כדי ללכוד נתוני מסגרות, Network Monitor ומנהל ההתקן של Network Monitor חייבים להיות מותקנים על מחשב Windows 2000. מנהל ההתקן של Network Monitor מאפשר ל-Network Monitor לקבל מסגרות ממתאם רשת. מסנן לכידה פועל כמו שאילתה למסד נתונים. ניתן להשתמש בו לציון סוגי מידע הרשת שרוצים לנטר. כדי לפשט את ניתוח הנתונים, Network Monitor מפענח נתונים גולמיים שנאספו בלכידה ומציג אותם בחלון Frame Viewer. ניתן להשתמש במסנן תצוגה לציון איזה מידע רוצים להציג בחלון Frame Viewer. כמו מסנן לכידה, מסנן תצוגה פועל כמו שאילתה למסד נתונים, ומאפשר לבודד סוגים מסוימים של מידע.

שיעור 5:
Task Manager

Task Manager (מנהל המשימות) של Windows מספק תמצית מידע אודות ביצועי מחשב, בנוסף לתוכניות והליכים הפועלים על המחשב. על ידי שימוש ב-Task Manager ניתן לסיים תוכניות או הליכים, להפעיל תוכניות ולהציג תצוגה דינמית של ביצועי המחשב.

לאחר שיעור זה, תוכל

- להשתמש ב- Task Manager לניהול יישומים ומשימות.
- להשתמש ב- Task Manager להצגת ביצועי המחשב.

זמן לימוד משוער: 20 דקות

סקירה כללית של Task Manager

Task Manager (מנהל המשימות) מספק מידע אודות תוכניות והליכים הרצים על המחשב. הוא מציג גם את מידות הביצועים הנפוצות ביותר עבור הליכים.

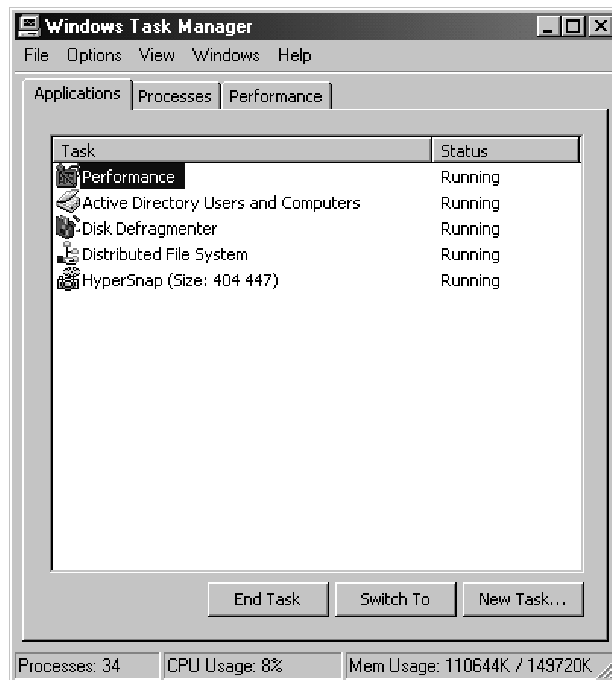
ניתן להשתמש ב-Task Manager לניטור מחוונים עיקריים של ביצועי המחשב. ניתן לראות במהירות את מצב התוכניות הפועלות, ולסיים תוכניות שהפסיקו להגיב. ניתן גם להעריך את הפעילות של הליכים בפעולה, על ידי הצגת נקודות נתונים קריטיות רבות, וניתן להציג גרפים ונתונים אודות שימוש במעבד ובזיכרון.

לפתיחת Task Manager, לחץ לחיצה ימנית על מקום ריק כלשהו בשורת המשימות (Taskbar) ואז לחץ על Task Manager. ניתן גם לפתוח את Task Manager על ידי הקשה על Ctrl+Alt+Del ואז לחיצה על לחצן Task Manager. ממשק Task Manager כולל שלוש כרטיסיות: Applications, Processes ו-Performance (יישומים, הליכים וביצועים). ניתן לשנות את אפשרויות התצוגה עבור כל כרטיסיה, על ידי בחירת האפשרות הרצויה מתפריט View. רבות מהאפשרויות בתפריט View הן ייחודיות לכרטיסיה שנבחרה.

לעדכון נתוני Task Manager, בחר את Refresh Now בתפריט View. ניתן גם לשנות את התדירות בה מעודכנים הנתונים אוטומטית. בתפריט View, לחץ על Update Speed, ואז לחץ על האפשרות הרצויה. להקפאה זמנית של הנתונים המוצגים על ידי Task Manager, לחץ על Update Speed בתפריט View, ואז לחץ על Paused.

הכרטיסיה Applications

הכרטיסיה Applications מציגה את מצב התוכניות הפועלות על המחשב (תרשים 13.17). בכרטיסיה זו, ניתן להתחיל תוכנית חדשה (לחצן New Task), לסיים תוכנית (לחצן End Task), או לעבור לתוכנית אחרת (לחצן Switch To).

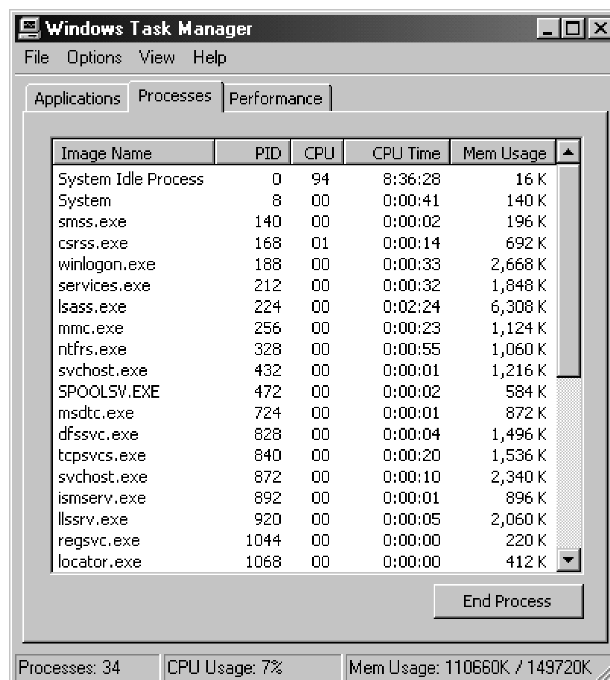


תרשים 13.17 הכרטיסיה Applications של Task Manager.

שימוש ב- Task Manager להפעלת תוכנית זהה לשימוש בפקודה Run בתפריט Start. אם תוכנית מפסיקה להגיב, לחץ על Alt+Ctrl+Del להפעלת Task Manager, בחר את התוכנית שאינה מגיבה, ולחץ End Task. נתונים כלשהם שהוזנו או שינויים כלשהם שבוצעו ואשר לא נשמרו, יאבדו.

הכרטיסיה Processes

הכרטיסיה Processes מציגה מידע אודות ההליכים הפועלים על המחשב (תרשים 13.18). לדוגמה, ניתן להציג מידע אודות שימוש במעבד ובזיכרון, תקלות החלפה, מוני טיפול ומספר פרמטרים אחרים.



תרשים 13.18 הכרטיסיה Processes של Task Manager.

בכרטיסיה Processes, ניתן למיין את רשימת ההליכים ולהציג מוני הליך אחרים. תיאור של כל סוג מונה אותו ניתן לנטר, ניתן למצוא בעזרה של Task Manager. כדי לראות את מוני ההליך הזמינים, בחר בכרטיסיה Processes ואז בחר Select Columns מתפריט View.

ניתן גם לסיים הליך בכרטיסיה Processes. אולם, יש להיזהר בעת סיום הליכים. אם מסיימים יישום, הנתונים שלא נשמרו - יאבדו. אם מסיימים שירות מערכת, ייתכן שחלק כלשהו של המערכת לא יפעל כראוי.

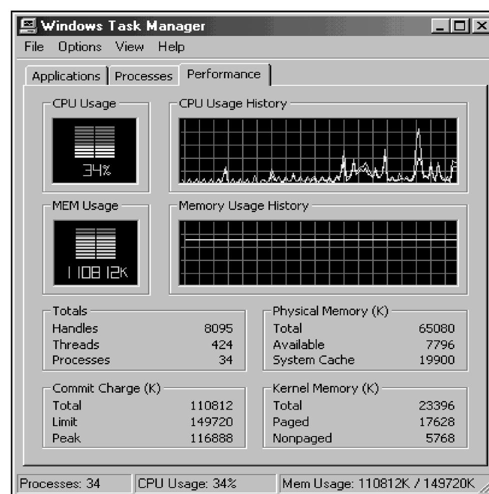
הערה Task Manager **אינו** מאפשר לסיים הליך שהוא קריטי לפעולת Windows 2000. תוכניות שירות ב- Windows 2000 Resource Kit **יאפשרו** לסיים הליכים קריטיים. אולם, פעולה זו עלולה לגרום לחוסר יציבות של מערכת ההפעלה.

ניתן לסיים הליך ואת כל ההליכים שנוצרו על ידו באופן ישיר או עקיף. לחץ לחיצה ימנית על ההליך שברצונך לסיים, ואז לחץ על End Process Tree. לדוגמה, אם מסיימים את עץ ההליכים עבור תוכנית דואר אלקטרוני כגון Microsoft Outlook 98, יסתיימו גם הליכים קשורים, כגון mapisp32.exe וה- MAPI spooler.

הכרטיסיה Processes גם מאפשרת להקצות הליך למעבד מסויים באמצעות הפקודה Set Affinity (הגדר קירבה/שיוך). פקודה זו זמינה רק במחשבים בעלי מספר מעבדים. שימוש בפקודה Set Affinity מגביל את ביצוע ההליך למעבדים שנבחרו, ועלול להפחית את הביצועים הכוללים. בנוסף, הכרטיסיה Processes מאפשרת לשנות את העדיפות של תוכנית פעילה. שינוי העדיפות של הליך יכול לגרום לו לפעול מהר יותר או לאט יותר, בהתאם לכיוון שינוי העדיפות, מעלה או מטה, ושינוי זה עלול גם להשפיע לרעה על הביצועים של הליכים אחרים. אם התקנת תוכנת ניפוי (Debugger), ניתן להפעיל את הפקודה Debug ישירות מתפריט הקיצור של ההליך הפעיל, המוצג תחת הכרטיסיה Processes.

הכרטיסיה Performance

הכרטיסיה Performance מציגה סקירה כללית דינמית של ביצועי המחשב (תרשים 13.19). תצוגה זו כוללת גרפים של שימוש במעבד ובזיכרון, סיכומים של מספר המזהים הייחודיים, הליכי המשנה, הליכים הפועלים על המחשב, וסיכומים ב- KB של זיכרון פיסי, זיכרון kernel ו-commit.



תרשים 13.19 הכרטיסיה Performance של Task Manager.

אם בוחרים את האפשרות Show Kernel Times מהתפריט View, מוצג קו אדום על גרף CPU Usage ועל גרף CPU Usage History. הקווים האדומים מציינים את כמות משאבי המעבד שנצרכו על ידי פעולות Kernel.

סיכום שיעור

Task Manager מספק מידע אודות תוכניות והליכים הפועלים על המחשב. הוא מציג גם את מידות הביצועים הנפוצות ביותר עבור הליכים. ממשק Task Manager מכיל שלוש כרטיסיות: Applications, Processes ו-Performance. הכרטיסיה Applications מציגה את מצב התוכניות הפועלות על המחשב. הכרטיסיה Processes מציגה מידע אודות ההליכים הפעילים במחשב. הכרטיסיה Performance מציגה סקירה כללית דינמית של ביצועי המחשב.

שאלות סיכום

השאלות הבאות נועדו לחזק את הנושאים העיקריים שהוצגו בפרק זה. אם אינך מסוגל לענות לשאלה, עיין בשיעור המתאים ונסה לענות על השאלה שנית. תשובות לשאלות ניתן למצוא בנספח A. לנוחיותך מופיעות השאלות באנגלית ואחר כך בעברית.

1. You have used the Compact utility to compress the files contained in the Users subfolders on an NTFS partition. You have enabled the Folder Option, Display Compressed Files And Folders With Alternate Color. A week later you use Windows Explorer to see if files are being compressed. To your surprise, user account subfolders, located directly under the Users folder created after you ran the compress utility, are not compressed. Why did this happen and how can you fix it?
2. Your department has recently archived several GB of data from a computer running Windows 2000 Server to CD- ROMs. As users have added files to the server, you have noticed that the server has been taking longer than usual to gain access to the hard disk. How can you increase disk access time for the server?
3. You are the administrator for a computer running Windows 2000 Server that is used to store user 's home folders and roaming user profiles. You want to restrict users to 25 MB of available storage for their home folder while monitoring, but not limiting, the disk space used for the roaming user profiles. How should you configure the volumes on the server?
4. You notice that a new server is not performing as well as you expected. You need to obtain summary information on a server 's performance, and then you want to use a utility to obtain detailed reports of performance bottlenecks. After you have resolved the performance problem, what should you do to track the performance of the server as more users begin to access the server?
5. You want to filter out all network traffic except for traffic between two computers, and you also want to locate specific data within the packets. Which Network Monitor filter features should you specify?
6. You goal is to make sure that only two network management stations in your organization are able to communicate with the SNMP agents. What measures can you take when configuring the SNMP service to enhance security?

1. השתמשת בתוכנית השירות Compact לדחיסת הקבצים בתיקיות המשנה Users במחיצת NTFS. אפשרת את Folder Option ואת Display Compressed Files And Folders With Alternate Color. שבוע לאחר מכן אתה משתמש בסייר Windows לבדוק אם הקבצים נדחסים. להפתעתך, תיקיות משנה של חשבונות משתמשים, הממוקמות ישירות תחת התיקיה Users, ואשר נוצרו לאחר הפעלת תוכנית השירות לדחיסה, אינן דחוסות. מדוע זה קרה וכיצד ניתן לתקן זאת?

2. המחלקה שלך אחסנה בארכיון לאחרונה מספר GB של נתונים ממחשב המפעיל Windows 2000 Server, אל תקליטורים. ככל שמשתמשים הוסיפו קבצים לשרת, שמת לב שלוקח לשרת יותר זמן מהרגיל לגשת לדיסק הקשיח. כיצד ניתן לשפר את זמן הגישה לדיסק עבור השרת?

3. אתה מנהל של מחשב המפעיל Windows 2000 Server, המשמש לאחסון תיקיות הבית של משתמשים ופרופילים של משתמשים ניידים. ברצונך להגביל משתמשים ל- 25MB של אחסון זמין עבור תיקיית הבית שלהם, תוך ניטור, אך ללא הגבלה, של המקום בדיסק המשמש עבור פרופילי המשתמשים הניידים. כיצד עליך להגדיר את ה-volumes בשרת?

4. שמת לב ששרת חדש אינו מספק ביצועים כפי שהיה צפוי. עליך לקבל תמצית מידע אודות ביצועי השרת, ואז ברצונך להשתמש בתוכנית שירות לקבלת דוחות מפורטים של צווארי בקבוק בביצועים. לאחר שפתרת את בעיית הביצועים, מה עליך לעשות כדי לעקוב אחר הביצועים של השרת עם גידול מספר המשתמשים הניגשים לשרת?

5. ברצונך לסנן (לא לכלול) את כל תעבורת הרשת, מלבד תעבורה בין שני מחשבים, וברצונך גם לאתר נתונים מסוימים בתוך המנות. באיזה תכונות סינון של Network Monitor עליך להשתמש?

6. מטרתך לוודא שרק שתי תחנות ניהול רשת בארגון שלך יוכלו לתקשר עם סוכני SNMP. באיזה צעדים עליך לנקוט, בעת הגדרת שירות SNMP, כדי להגביר אבטחה?

פרק 14

שרתי יישומים של Windows 2000

אודות פרק זה

Windows 2000 Server תומכת במספר שירותים המרחיבים את פונקציונליות מערכת ההפעלה Windows 2000. פרק זה מתמקד באחדים משירותים אלה, הכוללים בין השאר את **I**nternet **I**nformation **S**ervices (IIS), שירותי Telnet ושירותי המסוף (Terminal Services). פרק זה גם מספק את המידע הדרוש ליישום כל אחד משירותים אלה בסביבת Windows 2000, וניהול שירות זה לאחר הפעלתו.

לפני שתתחיל

לביצוע השיעורים בפרק זה, נדרש:

- Server01 ו-Server02 המפעילים Windows 2000 Server.
- השלמת התרגילים בפרקים הקודמים.

שיעור 1: סקירת מאפייני Internet Information Services

Windows 2000 Server כולל גירסה מעודכנת של IIS (גירסה 5.0). IIS מפעיל שירותים ארגוניים (Enterprise Service) בתוך Windows 2000 ומשתמש בשירותים אחרים המסופקים על ידי Windows 2000, כגון שירותי אבטחה ו- Active Directory. IIS 5.0 משפר את האמינות, הביצועים, הניהול, האבטחה ושירותי היישומים של שרת אינטרנט. רבים משיפורים אלה נובעים מהאופן שבו IIS 5.0 משלב תכונות חדשות של מערכת ההפעלה ב- Windows 2000. שיעור זה מהווה סקירה כללית של IIS 5.0 ומסביר כיצד להתקין IIS ולהגדיר סביבת אינטרנט.

לאחר שיעור זה, תוכל

- להתקין IIS 5.0 ולהגדיר סביבת אינטרנט.

זמן לימוד משוער: 40 דקות

מבוא ל- Microsoft IIS גירסה 5.0

בעוד ש- IIS 4.0 התמקד באבטחה, ניהול, יכולת תכנות ותמיכה בתקני אינטרנט, גירסה 5.0 של IIS מסתמכת על יכולות אלו לאספקת סוג אתרי האינטרנט הדרוש בסביבת עסקים, שהיא יותר ויותר סובבת אינטרנט ואינטראנט. IIS 5.0 כולל שיפורים בארבעת התחומים הבאים: אמינות וביצועים, ניהול, אבטחה וסביבת יישומים.

אמינות וביצועים

ל-IIS 5.0 יש ביצועים טובים יותר והוא אמין יותר מהגרסאות הקודמות של המוצר, וזאת ממספר סיבות. פנימית, מהירות מנוע IIS 5.0 הוגברה באמצעות שיפורים בקידוד. התכונה החדשה Reliable Restart (אתחול מחדש אמין) מאפשרת למנהלי מערכת להפעיל מחדש את השרת במהירות. מעבר ליכולות טבעיות אלו, מציגה גירסה זו תכונות שבהן ניתן להשתמש לשיפור המהירות והאמינות של אתרי אינטרנט.

אחד מהשיפורים המשמעותיים יותר ב-IIS 5.0 הוא הוספה של הגנת יישומים באמצעות תמיכה ביישומי מאגר, שאינם בהליך ביצוע (Pooled, Out-Of-Process Applications). לשליטה טובה יותר בצריכת משאבים, תכונות מצערת (Throttling) חדשות (המבוססות על תכונת אובייקט מטלה, Job object, החדשה של Windows 2000) מקלות על מנהלים להקצות את כמות רוחב פס CPU הזמין להליכים, בנוסף לכמות רוחב פס הרשת הזמין לאתרים. בנוסף, תכונת שקעי אגירה (Socket Pooling) החדשה מאפשרת למספר אתרים בעלי יציאה משותפת גם לשתף מערכת שקעים (Sockets).

הגנה על יישומים

מרבית מערכות ההפעלה מתייחסות להליך כאל יחידת עבודה במערכת. שירותים ויישומים הם הליכים הפועלים באזורי זיכרון המוקצים על ידי מערכת ההפעלה לכל הליך. ב-IIS 5.0, הגנה על יישומים מתייחסת לאופן שבו מערכת ההפעלה מגינה על כל הליך יישום מפני הליכים אחרים בזיכרון. בגרסאות קודמות של IIS, כל יישומי ISAPI (Internet Server API), כולל טכנולוגיית ASP, שיתפו ביניהם את המשאבים והזיכרון של הליך השרת IIS. למרות שהדבר סיפק ביצועים מהירים, רכיבים לא-יציבים יכלו לגרום לשרת IIS להיתקע או ליפול, דבר שהקשה על פיתוח ואיתור תקלות ברכיבים חדשים. בנוסף, לא ניתן היה להסיר רכיבים בעת ביצוע הליך (In-Process), אלא אם השרת אותחל מחדש - פירוש הדבר היה ששינוי רכיבים קיימים היה משפיע על כל האתרים שהשתתפו באותו שרת IIS, בין אם הם הושפעו ישירות מהשדרוג או לא.

כשלב ראשון לקראת פתרון נושאים אלה, איפשר IIS 4.0 ליישומים לפעול כחלק מאותו הליך שרת IIS (Inetinfo.exe) או מחוץ-להליך, כלומר בהליך נפרד מהליך שרת IIS. DLLHost.exe פועל כיישום פונדקאי להליך שרת IIS, לניהול כל יישום מחוץ-להליך. יישומים מחוץ-להליך מופעלים בנפרד זה מזה, דבר שצורך הרבה זיכרון ופחות יעיל מהפעלה בתוך-הליך. ב-IIS 5.0, קיימת אפשרות שלישית: ניתן להפעיל יישומים בהליך במאגר (Pooled) הנפרד מהליך שרת IIS. גישה זו מאפשרת להפעיל יישומים הקשורים זה לזה יחד מבלי להשפיע לרעה על הליך שרת IIS. שלוש אפשרויות אלו מספקות רמות שונות של הגנה, שכל אחת מהן משפיעה על הביצועים. בידוד רב יותר עולה בביצועים איטיים יותר.

Reliable Restart

במקרה של כשל במערכת, אין ספק שחשוב מאוד שניתן יהיה להחזיר את IIS למצב פעיל, מהר ככל הניתן. בעבר, אתחול מחדש היה דרך מקובלת, אם כי לא אופטימלית, להפעיל מחדש את IIS. כדי להפעיל מחדש את IIS בצורה אמינה, המנהל היה חייב להפעיל מחדש ארבעה שירותים נפרדים לאחר כל עצירה, והיה צריך להיות בעל ידע מיוחד, כמו למשל איזה שירותים להפעיל ובאיזה סדר. כדי למנוע צורך זה, כוללת Windows 2000 את IIS Reliable Restart, הליך אתחול מחדש בשלב יחיד שהוא מהיר יותר, קל יותר וגמיש יותר.

Socket Pooling

IIS 5.0 מגביר ביצועים על ידי הוספת היכולת למיטוב גישה לאתר האינטרנט. שקע (Socket) הוא מזהה פרוטוקול עבור צומת מסוים ברשת. השקע כולל כתובת צומת ומספר יציאה, המזהה את השירות. לדוגמה, יציאה 80 בצומת אינטרנט מייצגת את שירות World Wide Web HTTP בשרת Web.

ב-IIS 4.0, כל אתר אינטרנט מקושר לכתובת IP שונה, כלומר לכל אתר יש שקע נפרד שאינו משותף עם אתרים המקושרים לכתובות IP שונות. כל שקע נוצר עם תחילת האתר וצורך לא מעט זיכרון RAM פיסי שאינו משתתף בהחלפה עם זכרון מדומה על הדיסק (Non-Paged RAM). צריכת זיכרון זו מגבילה את מספר האתרים המקושרים לכתובות IP, אותם ניתן ליצור על מכונה יחידה.

עבור IIS 5.0 הליך זה שונה כך שאתרים המקושרים לכתובות IP שונות, אך משתפים ביניהם את אותו מספר יציאה, יכולים כעת לשתף את אותה מערכת שקעים. התוצאה הסופית היא שניתן לקשר יותר אתרים לכתובת IP באותה מכונה, בהשוואה ל-IIS 4.0. ב-IIS 5.0, שקעים משותפים אלה משמשים באופן גמיש בין כל האתרים שהותחלו, ובכך פוחתת צריכת המשאבים.

אירוח מספר אתרים

לשיפור יכולת הגידול של IIS, תומכת Windows 2000 Server ביכולת לארח מספר אתרי אינטרנט על שרת יחיד. הדבר יכול לחסוך את הזמן והכסף הדרושים בתוך חברה שרוצה לארח אתרים שונים עבור מחלקות שונות, או עבור ספק שירותי אינטרנט המארח מספר אתרים עבור לקוחות שונים.

המפתח לאירוח מספר אתרים על שרת יחיד הוא היכולת להבחין ביניהם. הדבר ניתן לביצוע במספר דרכים, שכל אחת מהן משתמשת בזיהוי אתר האינטרנט. לכל אתר אינטרנט יש זיהוי ייחודי בן שלושה חלקים בו הוא משתמש לקבלה ולתגובה לבקשות: מספר יציאה, כתובת IP ושם כותרת מארח. בעזרת IIS 5.0, חברות יכולות לארח מספר אתרי אינטרנט על שרת יחיד, על ידי שימוש באחת משלוש שיטות: הקצאת יציאות שונות, הקצאת כתובות IP שונות, או הקצאת שמות כותרת מארח שונים. כל אתר אינטרנט יכול לשתף שניים מתוך שלושת המאפיינים הייחודיים, ועדיין להיות מזוהה כאתר ייחודי.

הערה IIS 4.0 מאפשר גם הוא לאחד מספר אתרי אינטרנט על שרת יחיד.

הגבלת זמן שימוש במעבד על ידי הליכים

אם מפעילים מספר אתרי אינטרנט המשתמשים בעיקר בדפי HTML על מחשב יחיד, או אם פועלים יישומים אחרים על אותו מחשב המשמש כשרת האינטרנט, ניתן להגביל את כמות זמן המעבד המותר לשימוש על ידי היישומים של אתר האינטרנט. כך ניתן להבטיח זמינות זמן מעבד עבור אתרי אינטרנט אחרים או עבור יישומים שאינם קשורים ל- IIS. הדבר נקרא Process Throttling.

הגבלת רוחב פס

אם חיבור הרשת או האינטרנט המשמש את שרת האינטרנט משמש גם שירותים אחרים כגון דואר אלקטרוני או חדשות, ייתכן שתרצה להגביל את רוחב הפס המשמש את שרת האינטרנט כדי לפנות רוחב פס לשירותים אחרים. Bandwidth Throttling (מצערת רוחב הפס) היא תכונה חשובה ב-IIS 5.0, המאפשרת למנהלים לווסת את רוחב פס השרת המשמש כל אתר על ידי הפעלת מצערת (הגבלה) של רוחב הפס הזמין עבור כרטיס הרשת. לדוגמה, הדבר מאפשר לספק שירותי אינטרנט להבטיח כמות קבועה מראש של רוחב פס עבור כל אתר.

הערה IIS 4.0 מאפשר הפעלת מצערת (הגבלה) של רוחב פס לפי אתר אינטרנט.

ניהול

בעוד ש-IIS 4.0 הציג מספר משמעותי של טכנולוגיות חדשות, יעד תכנון עיקרי עבור IIS 5.0 היה לגרום לשרת אינטרנט להיות קל יותר לשימוש על ידי המנהלים. לדוגמה, חלק מהמנהלים התקשו בהתקנת IIS 4.0. בעזרת IIS 5.0, הליך ההתקנה מובנה ישירות לתוך הגדרות Windows 2000 Server. בנוסף, כדי להקל על ביצוע הגדרות אבטחה, נוספו שלושה אשפי אבטחה חדשים. גירסה זו גם כוללת תסריטי ניהול משופרים משורת הפקודה בנוסף לתסריטי ניהול מובנים נוספים.

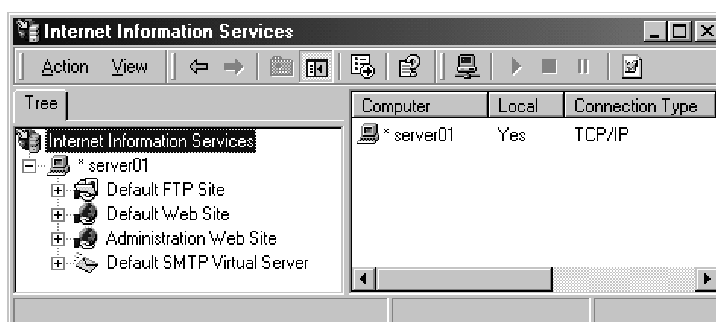
שילוב התקנה ושדרוג

הליך ההתקנה (Setup) של IIS 5.0 משולב עם התקנת Windows 2000 Server, ו-IIS 5.0 מותקן כברירת מחדל כרכיב Windows של Windows 2000 Server. באשף Windows Components, הוא רשום בשם **I**nternet **I**nformation **S**ervices (IIS). בעת התקנת מערכת ההפעלה, האשף מסייע להתקין עותק חדש של IIS 5.0 או לשדרג גירסה ישנה יותר.

כאשר מתקינים את Windows 2000 Server יוצר IIS אתר ברירת מחדל, אתר ניהול (Administration Site), ושרת SMTP וירטואלי ברירת מחדל (Default SMTP Virtual Server). ניתן להוסיף או להסיר את IIS או לבחור רכיבים נוספים, כגון שירות NNTP (**N**etwork **N**ews **T**ransfer **P**rotocol), על ידי שימוש ביישומון Add/Remove Programs שבלוח הבקרה. מ- Add/Remove Programs, הפעל את אשף Windows Components, ולחץ Details על הרכיב IIS.

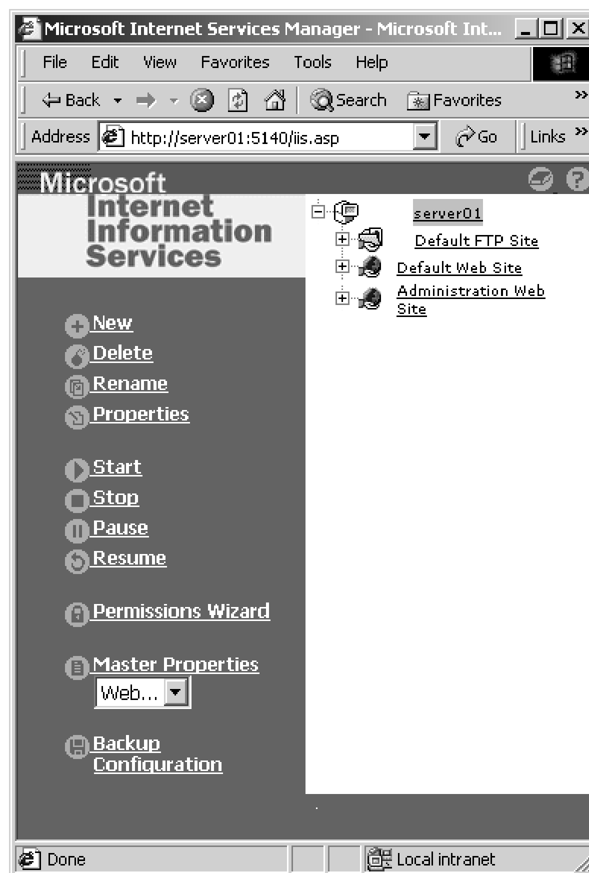
ניהול מרכזי

IIS 5.0 מנוהל על ידי שימוש בתוסף התוכנה Internet Information Services (תרשים 14.1), המשולב עם פונקציות ניהול אחרות של Windows 2000 (בגרסאות קודמות כלי זה נקרא Internet Service Manager). ניתן לגשת לתוסף התוכנה Internet Information Services דרך קבוצת התוכניות Administrative Tools. תוסף התוכנה Internet Information Services גם ממוקם בתוסף התוכנה Computer Management תחת Services and Applications.



תרשים 14.1 תוסף התוכנה Internet Information Services.

כלי הניהול מבוסס הדפדפן, Internet Services Manager (HTML), אינו זמין עוד בקבוצת התוכניות Administrative Tools, אולם הוא עדיין זמין, כדי לאפשר לנהל את IIS מרחוק, על פני חיבור HTTP או HTTPS, בהתאם לאופן בו הוגדרה האבטחה עבור אתר האינטרנט Administration. ניתן להפעיל את Internet Services Manager (HTML) על ידי בחירת צומת אתר האינטרנט Administration בחלון Tree של תוסף התוכנה Internet Information Services ואז ללחוץ על Browse מתוך התפריט Action. או שניתן לגשת אליו ישירות על ידי ציון שם השרת, מספר יציאת TCP המוקצה לאתר, וכתובת אתר האינטרנט Administration כמוצג בשדה Address בתרשים 14.2.



תרשים 14.2 ניהול IIS על Server01 ממחשב מרוחק.

הערה מספר יציאת TCP המוקצה לאתר הניהול נבחר באופן אקראי בין 2,000 ל- 9,999. הצג את תיבת הדו-שיח Properties של אתר האינטרנט Administration בכרטיסיה Web Site, כדי להגדיר או לשנות את מספר היציאה המוקצה לאתר.

ניתן להשתמש בדפדפן אחר מלבד Microsoft Internet Explorer לגישה לאתר האינטרנט Administration, אולם יש לאפשר Basic Authentication (אימות בסיסי) במידה והדפדפן אינו תומך באימות NTLM, ולא רוצים לאפשר גישה אנונימית. בנוסף, ניתן להשתמש בשירותי המסוף (Terminal Services) לניהול מרוחק של IIS באמצעות תוסף התוכנה Internet Information Services.

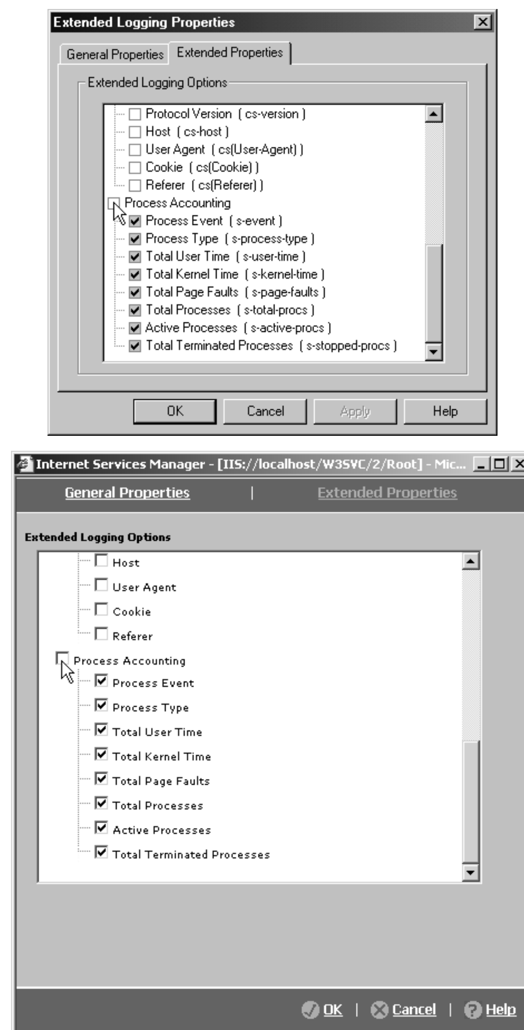
האצלת סמכויות ניהול

לסיוע בחלוקת עומס העבודה של משימות ניהול, יכולים מנהלים להוסיף חשבונות ניהול לקבוצה Operators. חברים בקבוצה Operators מקבלים הרשאות ניהול מוגבלות באתרי אינטרנט. לדוגמה, ספק שירותים שמארח אתרים עבור מספר חברות שונות יכול להאציל את סמכות הניהול לנציגים (Delegates) מכל חברה, כמפעילים של אתר האינטרנט של כל חברה. מפעילים יכולים לנהל מאפיינים המשפיעים על האתרים המסוימים שלהם בלבד. אין להם גישה למאפיינים המשפיעים על IIS, על מחשב שרת Windows המארח את IIS, או על הרשת. הדבר מאפשר למנהל טכנולוגיית המידע, או לספק שירותי אינטרנט המארח מספר אתרי אינטרנט על שרת יחיד, להעביר לנציגים את הניהול היומיומי של אתר האינטרנט מבלי לוותר על שליטה ניהולית כוללת.

Process Accounting

Process Accounting (המכונה לעתים CPU Usage Logging, CPU Accounting, או Job Object Accounting) הוא תכונה חדשה ב- IIS 5.0, המאפשרת למנהלים לנטר ולרשום יומן כיצד משתמשים אתרי אינטרנט במשאבי המעבד על השרת. ניהול חשבונות תהליכי מעבד מוסיף לקובץ היומן המורחב W3C שדות, לרישום מידע אודות האופן בו אתרי אינטרנט משתמשים במשאבי מעבד על השרת. ספקים של שירותי אינטרנט יכולים להשתמש במידע זה כדי לקבוע איזה אתרים משתמשים במשאבי מעבד באופן חריג, או שיש בהם תסריטים או הליכי CGI (**C**ommon **G**ateway **I**nterface) לא תקינים. מנהלי טכנולוגיית המידע יכולים להשתמש במידע זה לחיוב עלות האירוח של אתר האינטרנט או היישום מול המחלקה המתאימה בחברה, או לקבוע כיצד לשנות את הקצאת משאבי מעבד או רוחב פס של ההליכים, לשליטה על ניצולת משאבים.

כדי לאפשר ניהול חשבון הליכי מעבד באתר המשתמש בתוסף התוכנה Internet Information Services, פתח את מאפייני האתר, ומהמאפיינים של W3C Extended Log File Format, בחר בכרטיסיה Extended Properties. בצע ניווט זהה ב- Internet Service Manager (HTML), ואז בחר את הקישור Extended Properties. תרשים 14.3 מציג את תיבת הדו-שיח Extended Logging Properties ואת דף האינטרנט Extended Logging Options.



תרשים 14.3 אפשור ניהול חשבונות תהליכי מעבד דרך תיבת הדו-שיח Extended Logging Properties או דרך דף האינטרנט Extended Logging Options.

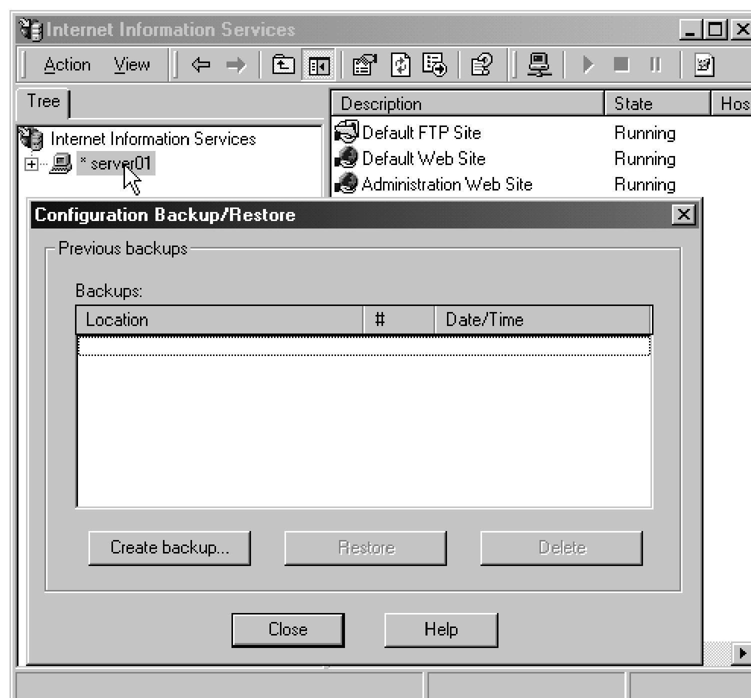
תסריטי ניהול משופרים משורת הפקודה

IIS 5.0 משווק עם תסריטים הניתנים להפעלה משורת הפקודה, לאוטומציה של ניהול משימות שרת אינטרנט נפוצות. תסריטים אלה ממוקמים בתיקיה \Inetpub\Scripts. תסריטי ניהול מאפשרים אוטומציה של חלק ממשימות הניהול הנפוצות ביותר. ניתן להשתמש בהם ליצירה ושליטה על אתרי אינטרנט, יישומים, ספריות ועוד. מנהלים גם יכולים ליצור תסריטים מותאמים אישית לאוטומציה של ניהול IIS. **W**indows **S**cript **H**ost (WSH) משמש להפעלת תסריטי הניהול vbs הכלולים ב- IIS 5.0.

גיבוי ושחזור IIS

תוסף התוכנה Internet Information Services מאפשר גם לגבות ולשחזר את תצורת IIS. כך, ניתן לשמור את הגדרת Metabase של IIS 5.0 כדי להקל על חזרה למצב ידוע ובטוח. על ידי שימוש בשיטה זו, ניתן לגבות ולשחזר את הגדרות שרת האינטרנט, אולם לא את קבצי התוכן או את אותן הגדרות הנשארות ברישום המערכת (Registry).

לגיבוי ושחזור תצורת שרת האינטרנט, בחר את מחשב ה- IIS בתוסף התוכנה Internet Information Services, ובחר את האפשרות Backup/Restore Configuration מתפריט Action. תוצג תיבת הדו-שיח Configuration Backup/Restore (תרשים 14.4), המאפשרת ליצור גיבוי, לשחזר גיבוי, או למחוק גיבוי שכבר נוצר.



תרשים 14.4 גישה אל תיבת הדו-שיח Configuration Backup/Restore עבור Server01.

הודעות שגיאה מותאמות אישית

כאשר משתמש מנסה להתחבר לאתר אינטרנט ומתרחשת שגיאת HTTP, נשלחת הודעה כללית בחזרה אל דפדפן הלקוח, עם תיאור קצר של מה שהתרחש בעת הניסיון ליצור חיבור. כמו ב- IIS 4.0, כך גם ב- IIS 5.0, ניתן לשלוח הודעות שגיאה המכילות יותר מידע ללקוחות הנתקלים בשגיאת ASP או HTML באתר. ניתן להשתמש בהודעות השגיאה המותאמות אישית המסופקות על ידי IIS 5.0, או ליצור אחרות.

ב-IIS 5.0 הודעות השגיאה המותאמות אישית מאוחסנות בתיקיה systemroot%\Help\iisHelp\common%. ב- IIS 4.0 הודעות השגיאה המותאמות אישית מאוחסנות בתיקיה systemroot%\Help\common%. הקידומת של קובץ הודעת שגיאה מותאמת אישית היא שם השגיאה, והסיומת היא htm. אם הודעת שגיאה מכילה נקודה, כמו למשל 403.3, שם קובץ הודעת השגיאה המותאמת אישית המתאים יכיל מקף, למשל 403-3.htm.

תמיכה בהרחבות שרת FrontPage

Windows 2000 Server מאפשרת למנהלים (Administrators) להשתמש בתכונות חיבור וניהול Web של FrontPage להפעלה וניהול אתרי אינטרנט. בעזרת FrontPage Server Extensions, יכולים מנהלים להציג ולנהל אתר אינטרנט בממשק גרפי. בנוסף, מחברים יכולים ליצור, לערוך ולפרסם דפי אינטרנט ל- IIS מרחוק. תוסף התוכנה FrontPage Server Extensions מאפשר לנהל את הרחבות השרת של FrontPage ואתרי אינטרנט שהורחבו על ידי FrontPage.

שלא כמו בגרסאות קודמות של IIS, FrontPage Web מופעל כברירת מחדל. ניתן לגשת לתוסף התוכנה FrontPage Extensions מתוך Server Extensions Administrator Console או מתוסף התוכנה Internet Information Services. שתי תכונות ההתקנה הבאות בתוסף התוכנה FrontPage Server Extensions חשובות להגדרה ובדיקה ראשוניות של ההרחבות:

- **הגדרת שרת אינטרנט קיים לשימוש בהרחבות השרת** – לאחר שאתר אינטרנט מוגדר לשימוש בהרחבות השרת, יישומי אינטרנט התלויים בהרחבות שרת, כגון FrontPage, יכולים לפעול על אתר האינטרנט.
- **בדיקה של אבטחת ההרחבה בשרת** – תכונה זו מאפשרת לבדוק את האבטחה של אתרי האינטרנט או אתר אינטרנט יחיד המפעיל Server Extensions.

בתוסף התוכנה Internet Information Services, הגדרת שרת אינטרנט קיים עבור הרחבות שרת מבוצעת על ידי בחירת אתר אינטרנט ואז, מהתפריט Action, הצבעה על New, ולחיצה על האפשרות Server Extensions. כדי לבדוק את אבטחת ההרחבה בשרת של כל אתרי האינטרנט, בחר Internet Information Services בחלון Tree ואז מהתפריט Action הצבע על All Tasks, ולחץ על Check Server Extensions. כדי לבדוק הרחבות שרת עבור אתר יחיד, בחר את האתר מחלון Tree, ובצע את אותם שלבים כמו עבור בדיקת כל האתרים.

ביזור כתיבה וגרסאות באמצעות האינטרנט

האינטרנט הוא כלי מעולה לפרסום מסמכים, אולם עד עתה לא היה קל לארגונים להשתמש באינטרנט כדי לאפשר למשתמשים לשתף פעולה על מסמכים. זאת מכיון שבעוד שהיה קל לקרוא מסמכים המאוחסנים באתר אינטרנט, לא היה קל למשתמשים לבצע שינויים באותם מסמכים. כדי לענות על צורך זה, IIS 5.0 מוסיף תמיכה מלאה ב- Web **D**istributed **A**uthoring and **V**ersioning (Web DAV).

על ידי הגדרת ספריית WebDAV על שרת האינטרנט, ניתן לאפשר למשתמשים לשתף מסמכים על פני האינטרנט, או על פני רשת אינטראנט. WebDAV ב- IIS 5.0 מנצל את תכונות האבטחה והגישה לקבצים המסופקות על ידי Windows 2000, כך שניתן לנעול ולפתוח משאבים כדי לאפשר למספר קבצים לקרוא קובץ, בעוד שרק אדם אחד בכל עת יכול לשנות את הקובץ. WebDAV נידון ביתר פירוט בשיעור 2 "ניהול סביבת אינטרנט".

מערכת קבצים מבוזרת

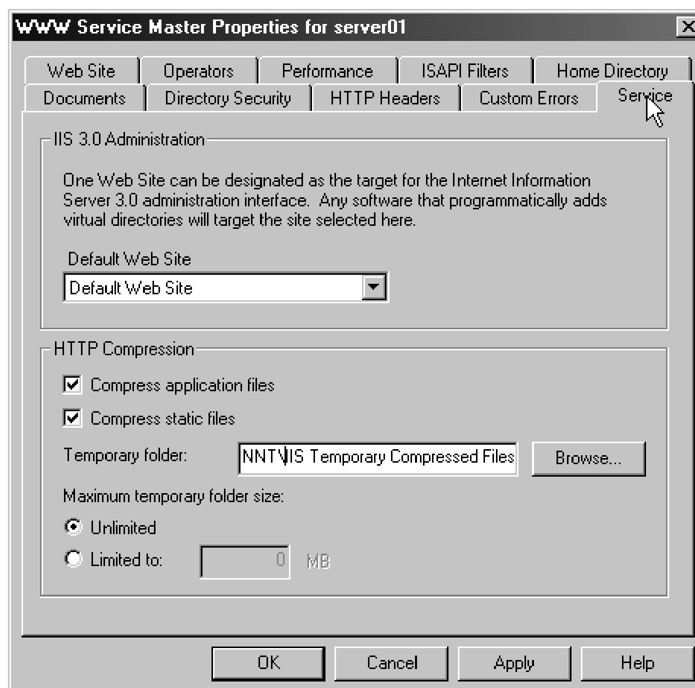
IIS 5.0 מנצלת את **מערכת הקבצים המבוזרת** (**D**istributed **F**ile **S**ystem - Dfs) של Windows 2000. Dfs היא אמצעי לאיחוד קבצים על מחשבים שונים לרשימת שמות יחידה. Dfs מאפשרת למנהלי מערכת לבנות תצוגה הירכית יחידה של מספר שרתי קבצים ושיתופי שרת קבצים על הרשת. כך קל יותר למשתמשים לגשת אל קבצים המבוזרים פיסית על פני הרשת ולנהל אותם. בעזרת Dfs, ניתן לגרום לקבצים המפוזרים על פני מספר שרתים להיראות למשתמשים, כאילו הם שוכנים במקום יחיד ברשת. משתמשים אינם צריכים עוד לדעת ולציין את המיקום הפיסי למעשה של קבצים כדי לגשת אליהם.

הערה למידע נוסף אודות Dfs, ראה פרק 5, שיעור 1.

דחיסת HTTP

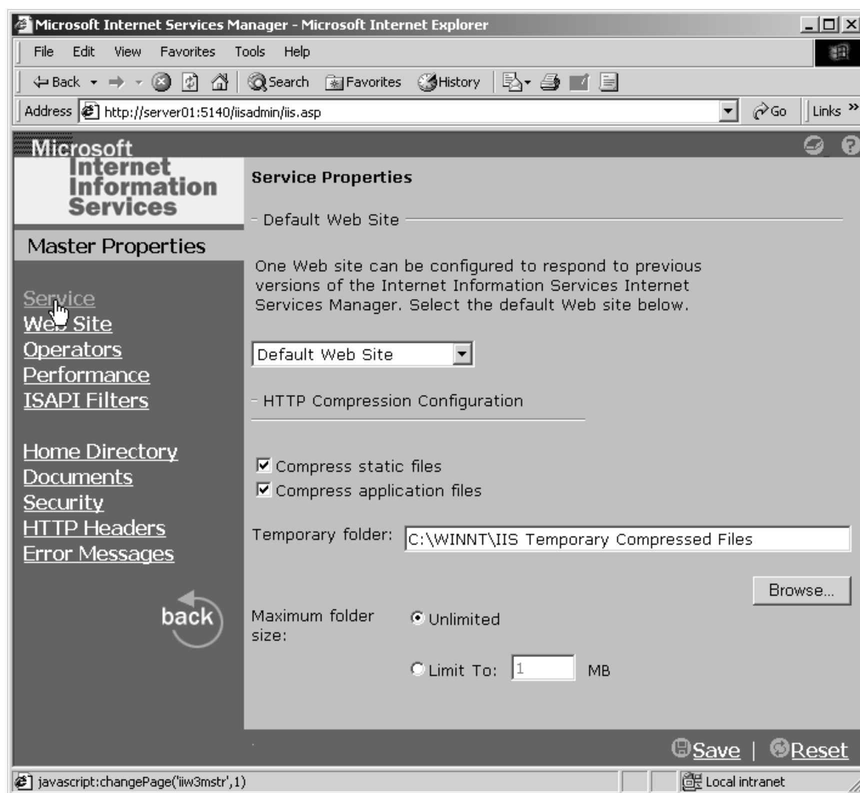
דחיסת HTTP מאפשרת העברה מהירה יותר של דפים בין שרת אינטרנט לבין לקוחות המאפשרים דחיסה. הדבר שימושי במצבים בהם רוחב הפס מוגבל. בהתאם לתוכן אותו מארחים, שטח האחסון הזמין, ומהירות הקשר של המבקר האופייני באתר האינטרנט, דחיסת HTTP יכולה לספק העברה מהירה יותר של דפים בין שרת האינטרנט ובין הדפדפן המאפשרות דחיסה.

בתוסף התוכנה Internet Information Services, דחיסת HTTP מתאפשרת מתוך המאפיינים העיקריים של הצומת Internet Information Services. בתיבת הדו-שיח Internet Information Services Properties, לחץ Edit, עבור WWW Service, ואז בחר בכרטיסיה Service (תרשים 14.5).



תרשים 14.5 WWW Service Master Properties for Server01 כפי שנראה מתוך תוסף התוכנה Internet Information Services.

מתוך דף הבית של Internet Information Service (HTML), לחץ Service תחת Master Properties. הצג את מאפייני השירות והגדר דחיסה (תרשים 14.6).



תרשים 14.6 WWW Service Master Properties for Server01 כפי שנראה מתוך הדף Internet Information Services Manager (HTML).

FTP ו- FTP Restart

שירות FTP, פרוטוקול תקני בענף המשמש לפרסום מידע אל שרת אינטרנט, משולב לתוך Windows 2000 Server. ב- IIS 5.0, הפרוטוקול FTP Restart נתמך גם הוא על ידי Windows 2000 Server. הוא מספק דרך מהירה וחלקה יותר להורדת מידע מהאינטרנט. אם מתרחשת הפרעה במהלך העברת הנתונים מאתר FTP, ההורדה יכולה להמשיך היכן שהפסיקה (Resume), בלי צורך להוריד מחדש את הקובץ כולו.

הערה תכונה זו זמינה רק עבור לקוחות FTP התומכים בפונקציה FTP Restart. לקוח FTP יוזם את הפקודה REST להתקשרות והמשך הורדה שכשלה.

אבטחה

תכונות אבטחה, שהן נושא חשוב בשיפורים של IIS 5.0, מנצלות את תכונות האבטחה בעלות תקן-אינטרנט, המשולבות לחלוטין עם Windows 2000.

תקני אבטחה

פרוטוקולי האבטחה הנתמכים על ידי IIS 5.0 מתוארים בטבלה הבאה.

אבטחה	תיאור פרוטוקול
Fortezza	התמיכה בתקן האבטחה של ממשל ארה"ב הנקרא Fortezza, היא תוספת חדשה ב- IIS 5.0. Fortezza מספק ארכיטקטורת אבטחת Defense Message System עם מנגנון קריפטוגרפי המספק סודיות הודעות, שלמות, אימות, אי-מניעה (Non-Repudiation) ובקרת גישה להודעות, רכיבים ומערכות. תכונות אלו ממומשות הן עם תוכנת שרת ודפדפן והן עם חומרת כרטיס PCMCIA.
Secure **S**ockets **L**ayer (SSL) 3.0	פרוטוקולי אבטחת SSL משמשים באופן נרחב בדפדפני אינטרנט ובשרתים לצורך אימות, שלמות הודעות, וסודיות. ניתן להגדיר את תוכנת מאפייני אבטחת SSL של שרת האינטרנט לוודא את שלמות התוכן, לוודא את זהות המשתמשים, ולהצפין תעבורת רשת. SSL מסתמך על תעודות (Certificates). ניתן להשתמש ב- Microsoft Certificate Services להנפקת תעודות. ראה פרק 11, שיעור 1 "תשתית המפתח הציבורי" למידע נוסף אודות תעודות ו- Certificate Services.
Transport **L**ayer **S**ecurity (TLS)	TLS מבוסס על SSL. הוא מאפשר אימות משתמשים קריפטוגרפי ומספק דרך למתכנתים עצמאיים לכתוב קוד מאופשר-TLS שיכול להחליף מידע קריפטוגרפי עם הליך אחר ללא צורך של המתכנת להכיר את הקוד של מתכנת אחר. בנוסף, מיועד TLS לספק מסגרת שיכולה לשמש מפתח ציבורי חדש ושיטות הצפנה גולמיות עם התהוותן. TLS גם מתמקד בשיפור ביצועים, על ידי הפחתת תעבורת רשת ואספקת שיטה חליפית לשמירת מטמון session, שיכולה להפחית את מספר החיבורים שיש להקים מאפס.
PKCS #7	פרוטוקול זה מתאר את התבנית של נתונים מוצפנים, כגון חתימות דיגיטליות או מעטפות דיגיטליות. שני אלה קשורים בתכונות התעודות של IIS.
PKCS #10	פרוטוקול זה מתאר את התבנית של בקשות לתעודות המוגשות לרשויות רישוי (**C**ertification **A**uthorities - CA).

אבטחה	תיאור פרוטוקול
Basic Authentication	Basic Authentication הוא חלק ממפרט HTTP 1.0. הוא שולח סיסמאות על פני רשתות בתבנית מקודדת Base64. שיטת Base Authentication זו היא תקן ענף בשימוש נרחב לאיסוף מידע שם משתמש וסיסמה. היתרון ב- Basic Authentication הוא שזהו חלק ממפרט HTTP, והוא נתמך על ידי מרבית הדפדפנים. החיסרון הוא שדפדפנים ברשת המשתמשים ב- Basic Authentication משדרים סיסמאות בתבנית לא-מוצפנת. על ידי האזנה לתקשורת ברשת, ניתן בקלות לקלוט ולפענח סיסמאות אלו, על ידי שימוש בכלים הזמינים לציבור. לכן, Basic Authentication אינו מומלץ - אלא אם אתה בטוח שהחיבור בין המשתמש לשרת האינטרנט מאובטח, עם חיבור כבל ישיר, קו ייעודי, או רשת אינטראנט בטוחה.
Digest authentication	Digest Authentication, תכונה חדשה של IIS 5.0, מציעה תכונות דומות לאלו של Basic Authentication, אולם כרוכה בשיטה אחרת להעברת פרטי האימות. פרטי האימות עוברים דרך הליך חד-כיווני, הנקרא במקרים רבים Hashing (תמצית הודעה/ערבול). תוצאת הליך זה נקראת Hash (ערבול), או Message Digest (תמצית הודעה), ולא ניתן לפענח את הטקסט המקורי מתוך Hash זה. השרת מייצר מידע נוסף המתוסף לסיסמה לפני Hashing, כדי שלא ניתן יהיה ללכוד את Hash הסיסמה ולהשתמש בו כדי להתחזות ללקוח האמיתי. זוהי מתודולוגיית סיסמה סודית משותפת. לשיטה זו יש יתרון ברור ביחס ל- Basic Authentication, בה גורם לא מורשה יכול ללכוד את הסיסמה ולהשתמש בה. Digest Authentication בנויה כך שניתן להשתמש בה על פני שרתי Proxy ויישומי FireWall אחרים, והיא זמינה ל- WebDAV. כיון ש- Digest Authentication היא תכונת HTTP 1.1 חדשה, לא כל הדפדפנים תומכים בה. אם דפדפן שאינו תואם מגיש בקשה לשרת הדורש Digest Authentication, השרת ידחה את הבקשה, וישלח ללקוח הודעת שגיאה. התמיכה ב- Digest Authentication היא עבור תחומי Windows 2000 בלבד, ו- Internet Explorer בגירסה 5 או מאוחרת יותר, הוא אחד מהדפדפנים הבודדים התומכים בתכונה זו.
Integrated Windows Authentication	שיטת אימות זו מספקת אימות Windows NT) NTLM Challenge/Response) עבור גרסאות ישנות יותר של Internet Explorer 3.0 המשתמשות בה לאימות קריפטוגרפי עם IIS. Integrated Windows Authentication גם מספקת לאתרי אינטרנט ולגרסאות חדשות יותר של Internet Explorer את אימות Kerberos v5. Integrated Windows Authentication משמש רק אם לא הופעלה, או שנדחתה גישה Anonymous כתוצאה מהגבלות הרשאות NTFS. Integrated Windows Authentication אינה נתמכת על פני חיבורי שרתי Proxy.

מנגנוני אבטחה

IIS 5.0 משתמש בחמישה מנגנוני אבטחה בסיסיים: אימות, תעודות, בקרת גישה, הצפנה וביקורת.

אימות

אימות (Authentication) מאפשר לוודא את הזהות של כל אחד המבקש גישה לאתרי האינטרנט. IIS תומך בסוגי האימות הבאים עבור שירותי HTTP ו-FTP:

- ❖ אימות FTP ו-HTTP אנונימי.
- ❖ אימות FTP ו-HTTP בסיסי.
- ❖ אימות Digest עבור תחומי Windows 2000 ודפדפנים התומכים בשיטת אימות HTTP 1.1 זו.
- ❖ אימות Integrated Windows (HTTP בלבד).

תעודות

להשלמת הליך האימות, נדרש מנגנון לוידוא זהויות משתמשים. תעודות (Certificates) הן מסמכי זיהוי דיגיטליים, המאפשרים הן לשרתים והן ללקוחות לאמת זה את זה. הן דרושות עבור השרת ודפדפן הלקוח להקמת חיבור SSL שעל פניו ניתן לשלוח מידע מוצפן. תעודות שרתים מכילות בדרך כלל מידע אודות החברה ואודות הארגון שהנפיק את התעודה. תעודות לקוח מכילות בדרך כלל מידע מזהה אודות המשתמש ואודות הארגון שהנפיק את התעודה.

בקרת גישה

לאחר וידוא זהות המשתמש, רוצים לשלוט על הגישה שלו למשאבים בשרת. IIS 5.0 משתמש בשתי שכבות של בקרת גישה (Access Control): הרשאות אינטרנט, והרשאות NTFS. הרשאות אינטרנט חלות על כל לקוחות HTTP ומגדירות גישה למשאבי שרת. הרשאות NTFS מגדירות את רמת הגישה של חשבונות משתמש בודדים לתיקיות וקבצים על השרת.

הצפנה

לאחר הבקרה על גישה למידע, יש להגן על מידע זה בעת העברתו על פני האינטרנט. ניתן לאפשר למשתמשים להחליף מידע פרטי, כגון מספרי כרטיס אשראי או מספרי טלפון, עם השרת בדרך מאובטחת על ידי שימוש בהצפנה. הצפנה (Encryption) מערבלת את המידע לפני שליחתו, ופענוח (Decryption) מפענח ערבול זה עם קבלת המידע. היסוד להצפנה זו הוא פרוטוקול SSL 3.0 ופרוטוקול TLS 1.0 המתהווה, המספקים דרך בטוחה להקמת חיבור תקשורתי מוצפן עם משתמשים. SSL מאשר את

אמיתות אתר האינטרנט, ויכול גם לאשר את זהות המשתמשים הניגשים לאתרי אינטרנט מוגבלים.

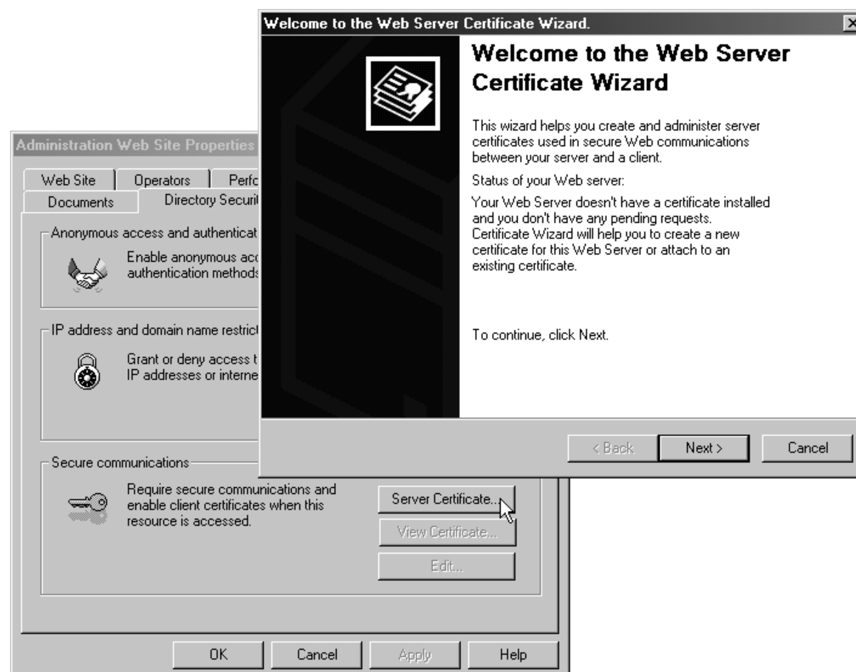
ביקורת

השלב האחרון להבטחת אבטחה הוא ניטור סדיר של השימוש באתר. מנהלים יכולים להשתמש בשיטת ביקורת אבטחה לניטור מיגוון רחב של פעילות אבטחה של המשתמשים ושרתי האינטרנט. ביקורת (Auditing) כוללת יצירת מדיניות ביקורת עבור גישה לתיקיות ולקבצים או אירועי שרת, וניטור יומני האבטחה לזיהוי ניסיונות גישה כלשהם על ידי אנשים בלתי מורשים. למידע נוסף אודות ביקורת, ראה פרק 11 בשיעור 5 "ביקורת Windows 2000".

אשפי אבטחה

כדי להקל על הקמה ותחזוקת הגדרות אבטחה, כולל IIS 5.0 שלושה אשפי משימות אבטחה חדשים: Web Server Certificate, Permissions, ו- Certificate Trust Lists.

האשף Certificates מפשט את משימות אימות התעודות, כמו למשל יצירת בקשות לתעודה וניהול מחזור החיים (Life Cycle) של התעודה. האשף Web Server Certificate מופעל באמצעות הלחצן Server Certificate במאפייני אתר אינטרנט, בתוסף התוכנה Internet Information Services.



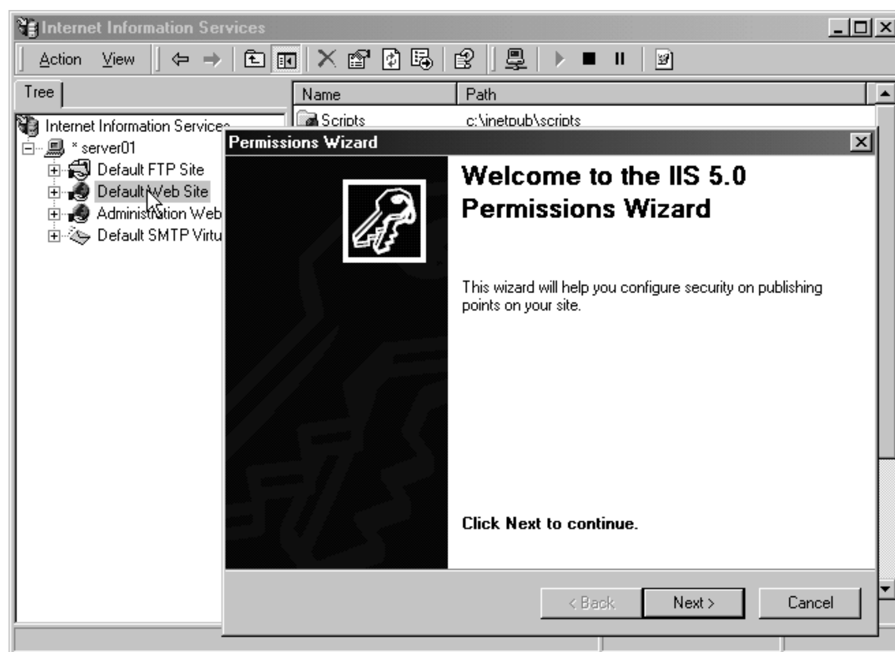
תרשים 14.7 הפעלת האשף Web Server Certificate מדף Properties של אתר האינטרנט Administration.

הערה שימוש ב- (HTML) Internet Information Services ליצירת תעודת שרת אינטרנט, דומה לשימוש בתוסף התוכנה Internet Information Services; אולם, אין כל אשף מבוסס HTML המסייע לאורך הליך הגדרות התצורה.

אבטחת SSL היא דרישה הולכת ונפוצה עבור אתרי אינטרנט המספקים מסחר אלקטרוני וגישה למידע עסקי רגיש. האשף החדש מקל על הקמת אתרי אינטרנט תואמי SSL על מחשב Windows 2000. בנוסף, אשף זה מסייע בהקמה ותחזוקת הצפנת SSL ואימות תעודות לקוח.

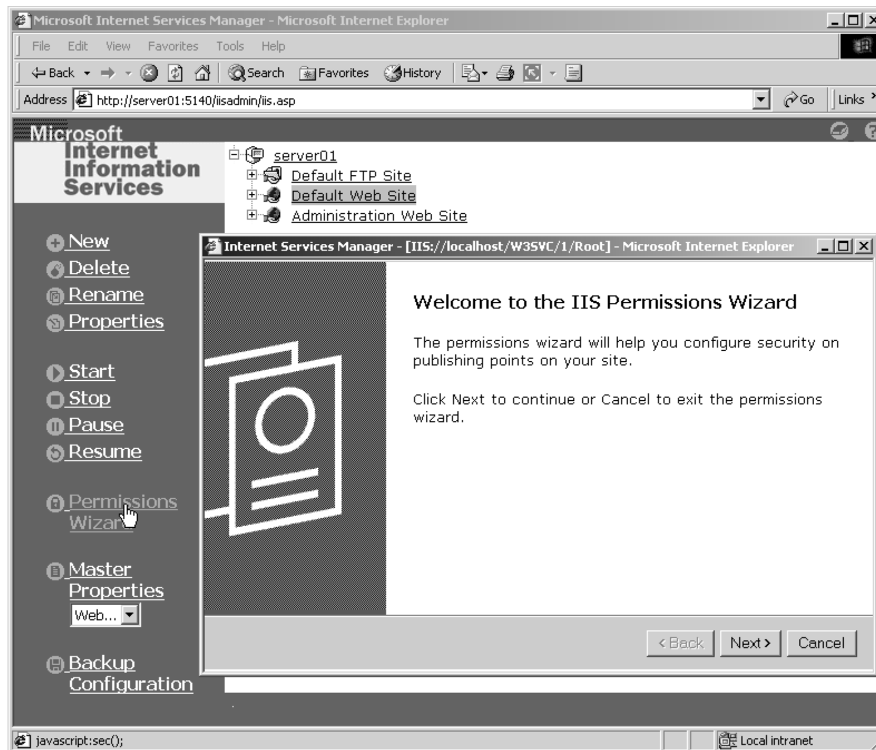
האשף Permissions מלווה מנהלים במשימות הגדרת הרשאות וגישה מאומתת באתר אינטרנט IIS, על ידי הקלת הליך ההקמה והניהול של אתר אינטרנט הדורש גישה מאומתת לתוכנו.

האשף Permissions מופעל מתוך תוסף התוכנה Internet Information Services. בחר אתר אינטרנט או אתר FTP. מהתפריט Action, הצבע על All Tasks ואז לחץ על Permissions Wizard. תרשים 14.8 מציג את מסך אשף Permissions המופעל מתוך תוסף התוכנה Internet Information Services.



תרשים 14.8 מסך Permissions Wizard מתוך אתר האינטרנט Default.

ניתן להפעיל את אשף Permissions גם מתוך (HTML) Internet Information Services, על ידי בחירת אתר אינטרנט או FTP מדף הבית, ואז לחיצה על הקישור Permissions Wizard במסגרת השמאלית של דף הבית, כמתואר בתרשים 14.9.



תרשים 14.9 מסך Permissions Wizard מבוסס HTML עבור אתר האינטרנט Default.

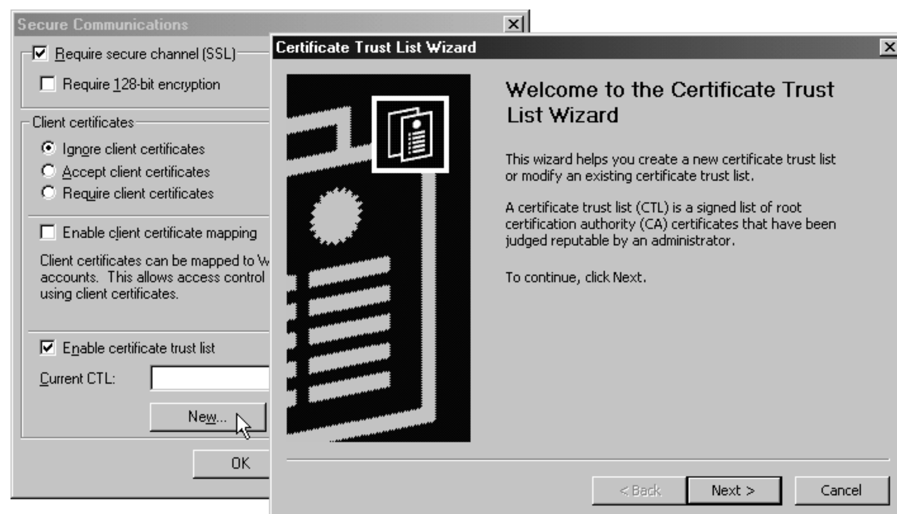
אשף Permissions מספק שתי אפשרויות ברמה העליונה:

- ❖ הגדרות אבטחה בירושה המוחלות על אתר האב או על ספריה וירטואלית.
- ❖ הגדרות אבטחה המבוססות על תבנית.

שתי תבניות זמינות להגדרת אבטחה: התבנית Public Web Site והתבנית Secure Web. התבנית Public Web Site מחילה הגדרות אבטחה, שהן תואמות בין דפדפנים ומספקות גישה לאתר ללא תלות בקיום חשבון Windows 2000 עבור המשתמש ברשת שאליה הוא ניגש. התבנית Secure Web Sits מחילה הגדרות אבטחה שרק משתמשים עם חשבונות משתמש Windows 2000 יכולים לגשת אליהן.

האשף Certificate Trust List מאפשר למנהלים להגדיר רשימות תעודות נאמנות - CTLs (**C**ertificate **T**rust **L**ists). CTL היא רשימה של רשויות הסמכה - CA (**C**ertification **A**uthorities) אמינות עבור ספריה מסוימת. רשימות אלו שימושיות במיוחד עבור ספקים של שירותי אינטרנט בעלי מספר אתרים על שרת אחד שצריכים רשימה שונה של CA מאושרים עבור כל אתר. רשימות CTL זמינות רק ברמת אתר האינטרנט ואינן זמינות עבור אתרי FTP.

לאחר הגדרת Server Certificate עבור אתר, מופעל אשף Certificate Trust List מהמאפיינים של אתר האינטרנט בתוסף התוכנה Internet Information Services. בכרטיסיה Directory Security של תיבת הדו-שיח Properties, לחץ על הלחצן Edit, תחת Secure Communications להצגת תיבת הדו-שיח Secure Communications. מתיבת דו-שיח זו, סמן את תיבת הסימון Enable Certificate Trust List, ואז לחץ New. יוצג האשף Certificate Trust List (תרשים 14.10).



תרשים 14.10 ניווט אל אשף Certificate Trust List לאחר הפעלת CTL.

ניתן גם לאפשר ולהגדיר CTL מ- Internet Service Manager (HTML), אולם אין אשף מבוסס HTML תואם. בנוסף, לא ניתן לערוך את התעודות דרך ממשק HTML, אולם ניתן לערוך את התעודות מתוך תוסף התוכנה Internet Information Services.

סביבת יישומים

IIS 5.0 כולל שיפורי ביצועים המקלים על פיתוח יישומים המתאימים לאינטרנט. טכנולוגיית **A**ctive **S**erver **P**ages (ASP) בתוך IIS, בשילוב עם שירותי גישת נתונים ורכיבים בתוך Windows 2000, מספקים סביבת יישומים עשירה.

בגירסה זו, שיפורים בבקרת זרימה וטיפול בתקלות, רכיבי Windows Script Host ושיפורים אחרים, גורמים ל- ASP להיות קל יותר לשימוש עבור כותבי תסריטים ואנשי פיתוח יישומי אינטרנט. בנוסף, תכונות כגון ASP ללא תסריט, כוונון עצמי של ASP, ואובייקטים משופרי ביצועים, בנוסף לשיפורים בתוך מערכת ההפעלה Windows 2000, יכולים להגביר את מהירות יישומי ASP.

ASP היא סביבת תסריטי צד-השרת שבה ניתן להשתמש ליצירה והפעלת יישומי שרת אינטרנט אינטראקטיביים ודינמיים. בעזרת ASP, ניתן לשלב דפי HTML, פקודות תסריט, ורכיבי COM (**C**omponent **O**bject **M**odel) ליצירת דפי אינטרנט אינטראקטיביים או יישומים מבוססי אינטרנט, שהם קלים להפעלה ושינוי. קיימות מספר תכונות ASP חדשות ב- IIS 5.0, כגון יכולות בקרת זרימה חדשות ותכונות טיפול בשגיאות שמקלות על כתיבה ושליטה על התנהגות יישומי אינטרנט. תכונות חדשות אחרות, כגון עיבוד ASP ללא תסריט, משפרות את הביצועים של דפי ASP.

Component Services

IIS 5.0 ו- Component Services (COM+) הכלולים ב- Windows 2000 Server פועלים יחד ליצירת ארכיטקטורה בסיסית לבניית יישומי אינטרנט. בגירסה 4.0 של IIS, סיפק **M**icrosoft **T**ransaction **S**erver (MTS) תמיכה בהעברות (Transactions). ב- IIS 5.0 ו- Windows 2000, Component Services מספק את כל תמיכת ההעברות של MTS, בנוסף למספר תכונות אחרות לפיתוח והפעלת רכיבים. IIS משתמש בפונקציונליות המסופקת על ידי Component Services לביצוע המשימות הבאות:

- בידוד יישומים להליכים נפרדים.
- ניהול תקשורת בין רכיבי COM (כולל אובייקטים מובנים של ASP).
- תיאום עיבוד העברות (Transactions) עבור יישומי Transactional ASP.

Active Directory Services

שירותי Active Directory ב- Windows 2000 Server משמשים לאחסון וניהול מידע אודות משאבים מרושתים. על ידי אספקת מאגר מרכזי עבור מידע חיוני, מפשטים שירותי Active Directory את ניהול הרשת, מקלים על משתמשים במציאת משאבים, ומקלים על אנשי פיתוח בכתיבת יישומים.

ADSI (Microsoft **A**ctive **D**irectory **S**ervice **I**nterfaces) הוא דגם שירות ספריה מבוסס COM, המאפשר ליישומי לקוח תואמי ADSI לגשת למיגוון רחב של פרוטוקולי ספריה שונים, כולל שירותי Active Directory, LDAP, ו- NDS, תוך שימוש במערכת ממשקים פשוטה וסטנדרטית. ADSI מסוכך על יישום הלקוח מפני פרטי היישום וההפעלה של מאגר הנתונים או הפרוטוקול הבסיסיים.

IIS מאחסן את מרבית הגדרות תצורת אתר האינטרנט ב- IIS Metabase. IIS חושף ממשק DCOM ברמה נמוכה המאפשר ליישומים לגשת ולבצע פעולות ב-Metabase. כדי להקל על הגישה ל-Metabase, IIS גם כולל ספק ADSI העוטף את מרבית הפונקציונליות המסופקת על ידי ממשק DCOM, וחושף אותו לכל יישום לקוח תואם ADSI.

הערה למידע נוסף אודות התכונות החדשות ב- IIS 5.0, ראה בתקליטור המצורף לספר זה (\chapt14\articles\IISover.doc).

התקנת IIS 5.0

Internet Information Services 5.0 הוא רכיב של מערכת ההפעלה Windows 2000. התקנה והסרת IIS מבוצעות באחת משלוש דרכים: בעת התקנה או שדרוג Windows 2000, על ידי שימוש ביישומון Add/Remove Programs שבלוח הבקרה, או באמצעות שימוש בקובץ unattended.txt, בעת התקנה אוטומטית.

בעת ביצוע התקנה חדשה של Windows 2000 Server, IIS מותקן כברירת מחדל. ניתן להסיר את IIS או לבחור רכיבי IIS להוספה או להסרה באמצעות היישומון Add/Remove Programs.

כאשר משדרגים מגירסה קודמת של NT אל Windows 2000, תוכנית ההתקנה Setup מנסה לזהות גירסה קודמת של IIS. אם היא מזוהה, אז IIS 5.0 מותקן, ולא ניתן למנוע שדרוג ל- IIS 5.0. אולם, IIS 5.0 לא יותקן אם לא זוהה IIS קודם.

בעת התקנת IIS 5.0, כשדרוג או כהתקנה נקייה, תוכנית ההתקנה מוודאת שהפרוטוקול TCP/IP מותקן. אם תוכנית ההקנה אינה מוצאת TCP/IP, היא מתקינה אותו באופן אוטומטי ומגדירה אותו לשימוש ב-DHCP.

במהלך התקנת IIS, נוצרים אתר האינטרנט Default, אתר האינטרנט Administration, שרת דואר וירטואלי Default SMTP ואתר Default FTP. ניהול אתרי האינטרנט ואתר FTP נידונים ביתר פירוט בשיעור 2 "ניהול סביבת אינטרנט".

הערה שרת הדואר הווירטואלי (Default SMTP Virtual Server) הוא מעבר להיקף הכשרה זו. SMTP מספק תמיכה באספקת הודעות דואר אלקטרוני אל יישומי אינטרנט ואינטראנט.

הגדרה של סביבת אינטרנט

בין אם האתר נמצא באינטרנט או באינטראנט, עקרונות אספקת התוכן זהים. מציבים את קבצי האינטרנט בתיקיות על השרת, כך שמשתמשים יכולים ליצור קשר HTTP ולראות את הקבצים בעזרת דפדפן. אולם מלבד אחסון קבצים על השרת, יש לנהל את אופן הפעלת האתר, ועוד יותר מכך את אופן התפתחות האתר.

כיצד מתחילים

יש להגדיר את אתרי האינטרנט על ידי ציון איזה תיקיות מכילות את המסמכים שרוצים לפרסם. שרת האינטרנט אינו יכול לפרסם מסמכים שאינם בתוך תיקיות מסוימות אלו. לכן, השלב הראשון בהפעלת אתר אינטרנט הוא לקבוע את אופן סידור הקבצים. אז ניתן להשתמש בתוסף התוכנה Internet Information Services, או בממשק (Internet Services Manager (HTML לזיהוי איזה תיקיות (הנקראות ספריות, Directories, בתוסף התוכנה ובממשק HTML), הן חלק מהאתר.

אם רוצים להתחיל מייד, מבלי ליצור מבנה תיקיות מיוחד, והקבצים ממוקמים כולם על אותו דיסק קשיח של המחשב המפעיל IIS, ניתן לפרסם את המסמכים מיידית על ידי העתקת קבצי האינטרנט לתיקיית הבית ברירת המחדל.

משתמשי האינטראנט יכולים לגשת לקבצים אלה בעזרת כל אחת מכתובות URL הבאות:

- http://<computer_name/file_name>
- http://<FQDN/file_name>
- http://<IP_address/file_name>

היכן ש- computer_name, FQDN, ו- IP_address מזהים את שרת האינטרנט.

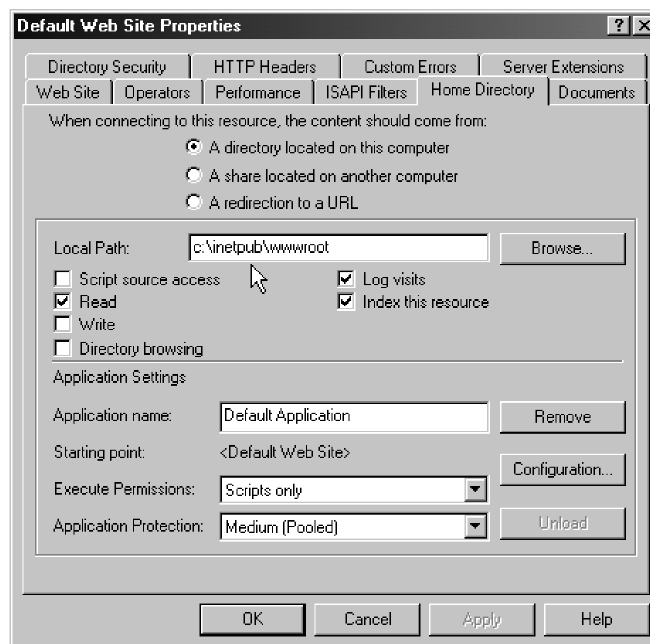
הערה בסעיף הבא, המילים **תיקיה ותיקיות** (Folder and Folders) מוחלפות במילים **ספריה וספריות** (Directory and Directories), מכיון שמשתמשים במילה Directory **ולא ב-** Folder בממשק Internet Information Services.

הגדרת ספריות בית

לכל אתר אינטרנט ואתר FTP חייבת להיות ספריית בית אחת. ספריית הבית היא המיקום המרכזי עבור הדפים המפורסמים. היא מכילה דף בית (שנקרא בדרך כלל index.htm, index.html, default.htm או default.html) המברך את משתמשי הדפדפן ומכיל קישורים לדפים אחרים באתר. ניתן להגדיר יותר ממסמך ברירת מחדל אחד עבור אתר יחיד. IIS מציג את מסמך ברירת המחדל הראשון שהוא מוצא. ספריית הבית ממופית אל שם ה-domain של האתר, או לשם השרת. לדוגמה, אם שם ה-domain של האתר הוא www.microsoft.com וספריית הבית היא C:\Website\Microsoft, הדפדפנים משתמשים בכתובת http://www.microsoft.com לגישה לקבצים בספריית הבית. ברשת אינטראנט, אם שם השרת הוא AcctServer, יכולים הדפדפנים להשתמש בכתובת http://acctserver לגישה לקבצים בספריית הבית.

ברירת מחדל של ספריית הבית נוצרת כאשר מתקינים את IIS וכאשר יוצרים אתר אינטרנט חדש. אם מגדירים גם אתר אינטרנט וגם אתר FTP על אותו מחשב, יש לציין ספריית בית אחרת עבור כל שירות (WWW ו-FTP). ברירת המחדל של ספריית הבית עבור שירות WWW היא InetPub\Wwwroot\. ברירת המחדל של ספריית הבית עבור שירות FTP היא InetPub\Ftproot\. ניתן לבחור ספריה אחרת כספריית הבית.

ניתן להשתמש בתוסף התוכנה Internet Information Services לשינוי ספריית הבית. בחר אתר אינטרנט או אתר FTP ופתח את תיבת הדו-שיח Properties שלו. בחר בכרטיסיה Home Directory, וציין את מיקום ספריית הבית (תרשים 14.11).



תרשים 14.11 הכרטיסיה Home Directory של תיבת הדו-שיח Default Web Site Properties.

אם בוחרים ספריה בשיתוף רשת, ייתכן שיהיה צורך להזין שם משתמש וסיסמה כדי לגשת למשאב. מומלץ להשתמש בחשבון IUSR_computername. אם משתמשים בחשבון שיש לו הרשאות ניהול על השרת, לקוחות יכולים לגשת לפעולות שרת. הדבר מסכן באופן משמעותי את אבטחת הרשת.

שים לב שספריית הבית יכולה להיות על המחשב המפעיל IIS, על שיתוף, או שניתן להפנות אותה אל URL המתארח באתר אינטרנט אחר. אפשרות השיתוף מספקת תמיכה שקופה ב-Dfs.

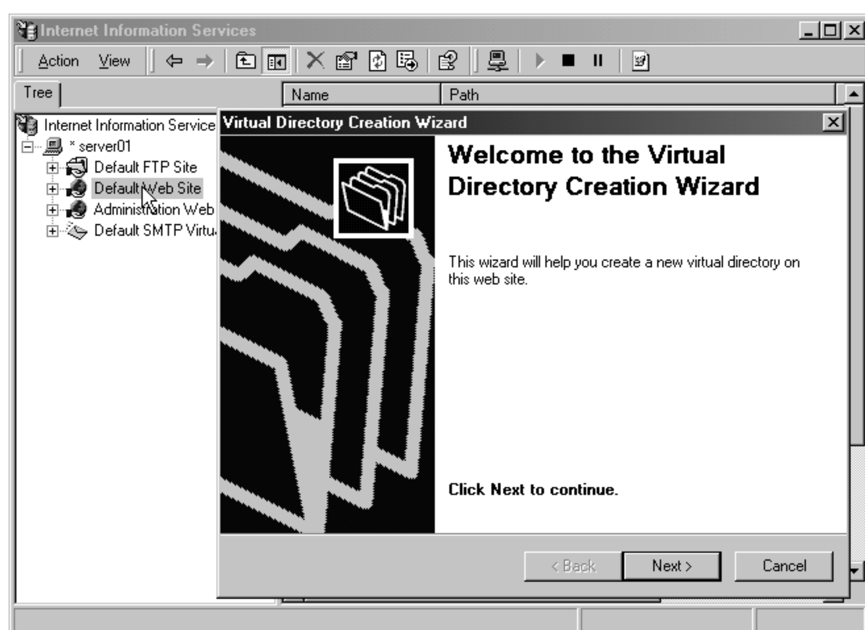
יצירת ספריות וירטואליות

ניתן ליצור ספריה וירטואלית לפרסום מספריה שאינה כלולה בספריית הבית. ספריה וירטואלית היא ספריה שאינה כלולה בספריית הבית, אולם נראית לדפדפני הלקוחות כאילו היא כן.

לספריה וירטואלית יש **כינוי** (Alias). שם בו משתמשים הדפדפנים, כדי לגשת לספריה זו. כיון שכינוי הוא בדרך כלל קצר יותר משם הנתיב עבור הספריה, הוא נוח יותר למשתמשים להקליד. כינוי גם בטוח יותר, כיון משתמשים אינם יודעים היכן הקבצים ממוקמים פיסית על השרת, ואינם יכולים להשתמש במידע זה לשינוי הקבצים. כינויים גם מקלים על הזזת ספריות באתר. במקום לשנות את כתובת URL של הספריה, ניתן לשנות את המיפוי בין הכינוי למיקום הפיסי של הספריה.

עבור אתר אינטרנט פשוט, ייתכן שלא יהיה צורך להוסיף ספריות וירטואליות. במקום זאת, ניתן להציב את כל הקבצים בספריית הבית של האתר. אם האתר מורכב, או שרוצים לציין כתובות URL שונות עבור חלקים שונים שלו, ניתן להוסיף ספריות וירטואליות לפי הצורך.

תוספי התוכנה Internet Information Services או Internet Services Manager (HTML) מאפשרים ליצור ספריה וירטואלית. בתוסף התוכנה Internet Information Services, בחר את אתר האינטרנט או אתר FTP אליו יש להוסיף ספריה וירטואלית. בתפריט Action הצבע על New, ולחץ על Virtual Directory. אשף Virtual Directory Creation מוביל אותך בהליך יצירת ספריה וירטואלית (תרשים 14.12).



תרשים 14.12 יצירת ספריה וירטואלית עבור אתר האינטרנט Default באמצעות אשף Virtual Directory Creation.

ב- Internet Services Manager (HTML), אותו קישור המשמש ליצירת אתר חדש, משמש גם לפרסום התוכן לספריה וירטואלית, או לספריה. לאחר בחירת אתר ב- Internet Services Manager (HTML) ולחיצה על הקישור New בחלונית השמאלית, יוצג האשף IIS New Site. במסך הבא באשף, ניתן לבחור את לחצן האפשרות Virtual Directory לפרסום ספריה וירטואלית חדשה.

ניתוב מחדש של בקשות בעזרת Redirects

כאשר דפדפן מבקש דף באתר האינטרנט, שרת האינטרנט מאתר את הדף המזוהה על ידי ה-URL ומחזיר אותו לדפדפן. כאשר מזיזים דף באתר האינטרנט, לא תמיד ניתן לתקן את כל הקישורים המפנים אל כתובת URL הישנה של הדף. כדי לוודא שדפדפנים יוכלו למצוא את הדף בכתובת החדשה, מורים לשרת האינטרנט לספק לדפדפן את כתובת URL החדשה. הדפדפן משתמש ב- URL החדש לבקש שוב את הדף. הליך זה מכונה **ניתוב מחדש של בקשת דפדפן** (Redirecting A Browser Request) או **ניתוב מחדש לכתובת URL אחרת** (Redirecting To Another URL). ניתוב מחדש של בקשה לדף דומה לשימוש בכתובת חדשה למשלוח דברי דואר. כתובת חדשה למשלוח מבטיחה שדברי דואר הממוענים לכתובת המקורית יועברו לכתובת החדשה.

ניתוב מחדש של URL שימושי בעת עדכון אתר אינטרנט, כשנדרש שחלק מהאתר לא יהיה זמין לפרק זמן כלשהו, או בעת שינוי שם של ספריה וירטואלית, כאשר נדרש שקישורים לקבצים בספריה הוירטואלית המקורית ייגשו אל אותם קבצים בספריה הוירטואלית החדשה.

ניתן להשתמש בתוסף התוכנה Internet Information Services לניתוב מחדש של בקשות לאתר אינטרנט, ספריה וירטואלית, או ספריה אחרת. בחר את אתר האינטרנט, הספריה הוירטואלית, או הספריה ופתח את תיבת הדו-שיח Properties המתאימה. עבור אתר אינטרנט, השתמש בכרטיסיה Home Directory; עבור ספריה וירטואלית, השתמש בכרטיסיה Virtual Directory; ועבור ספריה, השתמש בכרטיסיה Directory. בחר את האפשרות A Redirection To A URL, והקלד את URL היעד בתיבת הטקסט Redirect To.

כלים אחרים

במקרים רבים, ייתכן שיהיה שימושי לשנות תוכן Web באופן דינמי לאחר שהתבקש, אך לפני שהוחזר אל הדפדפן. IIS כולל שתי תכונות, המספקות תפקודיות כגון זו: **S**erver-**S**ide **I**ncludes (SSI) וסביבת תסריטי ASP.

על ידי שימוש ב- SSI, ניתן לבצע מיגוון רחב של פעילויות ניהול אתר אינטרנט החל מהוספת חותמת-זמן דינמית ועד להפעלת פקודת סביבה מיוחדת בכל פעם שמתבקש קובץ. פקודות SSI, הנקראות **הנחיות** (Directives), מוספות לדפי אינטרנט בשלב התכנון. כאשר דף מתבקש, שרת האינטרנט מנתח את כל ההנחיות שהוא מוצא בדף אינטרנט ומבצע אותן. SSI Directive נפוץ מוסיף, או כולל, את התוכן של קובץ לתוך דף אינטרנט. לדוגמה, אם יש צורך לעדכן ברציפות פרסומת בדף אינטרנט, ניתן להשתמש ב-SSI כדי לכלול את מקור HTML של הפרסומת לתוך דף האינטרנט. כדי לעדכן את הפרסומת, צריך רק לשנות את הקובץ המכיל את מקור HTML של הפרסומת. אין צורך להכיר שפת תסריטים לשימוש ב-SSI, נדרש רק להקפיד על כללי התחביר הנכון של ההנחיות.

ASP היא סביבת תסריטים של צד-השרת, בה ניתן להשתמש לשינוי דינמי של תוכן Web. למרות ש-ASP מתוכננת בעיקר לפיתוח יישומי אינטרנט, יש בה תכונות רבות שיכולות לשמש להקלה על ניהול אתרי אינטרנט. לדוגמה, בעזרת ASP ניתן לעקוב אחר משתמשים המשתמשים באתר האינטרנט, או להתאים אישית תוכן אתר, בהתאם ליכולות הדפדפן של הגולש באתר. אולם, שלא כמו SSI, ASP דורשת שימוש בשפת תסריטים כגון VBScript או JScript.

שימוש ב- ASP לניהול תוכן אתר אינטרנט

Windows 2000 כוללת את Microsoft ASP, סביבת תסריטים בצד השרת שבה ניתן להשתמש לאוטומציה וריכוז חלק ניכר ממשימות ניהול אתר אינטרנט.

תסריטים

תסריט הוא סדרת הוראות ופקודות, בהן ניתן להשתמש לשינוי מתוכנת של תוכן דפי האינטרנט. אם ביקרת פעם בחנות מקוונת, המאפשרת לחפש פריטים, ולבדוק זמינות מוצרים, אז אין ספק שנתקלת בסוג כלשהו של תסריט.

קיימים שני סוגי תסריטים: צד-לקוח (Client Side) וצד-שרת (Server Side). תסריטי צד-לקוח פועלים על הדפדפן ומשובצים בדף אינטרנט בין תגיות <SCRIPT> ו-</SCRIPT> של HTML. אם מציגים את מקור HTML של דף אינטרנט דינמי מאוד, קרוב לודאי שניתן למצוא שם תסריט צד-לקוח.

תסריטי צד-שרת פועלים באופן בלעדי על שרת האינטרנט, ומשמשים בדרך כלל לשינוי דפי אינטרנט לפני העברתם לדפדפן. תסריטי צד-שרת יכולים להורות לשרת האינטרנט לבצע פעולה, כגון עיבוד קלט ממשתמש או רישום מספר הפעמים שמשתמש מבקר באתר. ניתן לחשוב על תסריטי צד-שרת כמשפיעים על האופן בו מרכיב השרת דף אינטרנט לפני שליחתו לדפדפן. תסריטי צד-שרת יכולים בדרך כלל לאפשר ניהול תוכן אינטרנט, על ידי עיבוד נתונים ועדכון אוטומטי של דפי אינטרנט.

סקירה כללית של ASP

בדיוק כפי שניתן לכתוב פקודת מאקרו מותאמת אישית, לאוטומציה של גיליון נתונים מחזורי, או פעולות עיבוד תמלילים החוזרות על עצמן, ניתן ליצור תסריט צד-שרת לביצוע אוטומטי של משימות ניהול אינטרנט קשות, או החוזרות על עצמן. נניח שיש לעדכן אתר אינטרנט הכולל מספר עשרות עמודים המכילים מידע עיצוב זהה (כותרות משנה, לוגו של חברה, מידע זכויות יוצרים וכדומה). בדרך כלל, עבודה מסוג זה דורשת זמן רב ומחייבת עדכון (ובדיקה) של כל דף באופן ידני. אולם, ניתן להשתמש ב-ASP לאוטומציה של עבודה מסוג זה.

ASP היא סביבת תסריטים חזקה בצד השרת בה ניתן להשתמש לכתיבת תסריטים בעזרת עורך תמלילים סטנדרטי, כגון Notepad. לדוגמה, בעזרת ASP ניתן ליצור קובץ מרכזי המכיל מידע משותף לכל דפי אתר האינטרנט. בעת תכנון האתר, ניתן להוסיף פקודת תסריט בת שורה אחת לכל דף, המכניסה את תוכן הקובץ המרכזי. בכל פעם שצריך לעדכן את תפריט הניווט של האתר, לדוגמה, נדרש לעדכן את הקובץ המרכזי בלבד, שינויים יופיעו אוטומטית בפעם הבאה שמשתמש טוען מחדש ומציג את תוכן האתר.

ASP משתמשת ב**תוחמים** (Delimiters) להבחנה בין פקודות תסריט לבין טקסט רגיל ו-HTML. פקודות תסריט לביצוע על ידי השרת מוכלות בין תוחמים <% ו- %>, להבדיל מתוחמים < ו- > המשמשיםHTML לציון תגיות אותן צריך הדפדפן לנתח.

הדוגמה הבאה מציגה את אופן הפעולה של ASP:

```
<%
author = "Max"
department = "Quality Assurance"
%>
This page was updated <B>today</B>, by <%= author %> from the
<%= department %> Department.
```

כאשר דף זה מוצג בעזרת דפדפן, הוא ייראה כך:

This page was updated **today**, by Max from the Quality Assurance Department.

עם זאת, משתמש המציג את המקור של דף זה בדפדפן יראה רק את הטקסט ו- HTML כך:

This page was updated <B>today</B>, by Max from the Quality Assurance Department.

התסריט פועל על השרת (כלומר, פקודות בין התוחמים<% ו- %> מבוצעות על השרת) ומחזיר רק HTML אל הדפדפן של המשתמש.

קבצי ASP חייבים לכל הפחות להיות בעלי סיומת asp ולהכיל פקודות תסריט שנכתבו בשפת תסריטים כגון VBScript או JScript. אם נושא התסריטים חדש לך וברצונך ללמוד את היסודות, בקר באתר טכנולוגיות תסריטים של Microsoft, בכתובת http://msdn.microsoft.com/scripting/.

תרגיל 1: גישה לאתר האינטרנט Administration

בתרגיל זה תשתמש בתוסף התוכנה Internet Information Services להגדרת אתר האינטרנט Administration. תגדיר גישה לאזור רגיש זה של שרת האינטרנט. אחר כך תפעיל את Internet Service Manager (HTML) לבדיקת יכולת הגישה לאתר. בצע תרגיל זה על Server01.

הליך 1: הגדרת אתר האינטרנט Administration בעזרת תוסף התוכנה Internet Information Services

בהליך זה תשתמש בתוסף התוכנה Internet Information Services להגדרת אתר האינטרנט Administration.

1. היכנס ל- Server01 בשם משתמש Administrator עם סיסמה password.
2. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על Internet Services Manager. יופיע תוסף התוכנה Internet Information Services.
3. בחלון Tree, הרחב את server01 *

   ארבע מכולות יוצגו תחת server01 *, והן: Default FTP site ,Default Web site, Administration Web site, ו- Default SMTP Virtual Server.
4. בחלון Tree, הרחב את Administration Web site.

   שים לב שמופיעות שתי ספריות וירטואליות, IIS Admin ו- IIS Help.
5. בחלון Tree, לחץ על Administration Web site.
6. פתח את תפריט Action ולחץ Properties. תופיע תיבת הדו-שיח Administration Web Site Properties.
7. כאשר הכרטיסיה Web Site פעילה, רשום את ערך יציאת TCP המוצג בתיבת הטקסט TCP Port. לערך אקראי זה בין 2000 ל- 9999 נתייחס בהמשך תרגיל זה כמשתנה בשם **tcp_port**.
8. תחת תיבת הסימון Enable Logging, ודא שנבחר W3C Extended Log File Format ולחץ על הלחצן Properties.

   תופיע תיבת הדו-שיח Extended Logging Properties. שים לב שקובץ היומן מאוחסן בתיקיה %WinDir%\System32\LogFiles, שהיא המקבילה ל- %SystemRoot%\System32\LogFiles.
9. בחר בכרטיסיה Extended Properties.

10. גלול מטה לתחתית התיבה Extended Logging Options, וסמן את תיבת הסימון Process Accounting.

11. לחץ OK לסגירת תיבת הדו-שיח Extended Logging Properties. תופיע תיבת הדו-שיח Administration Web Site Properties.

12. בחר בכרטיסיה Directory Security.

13. באזור Anonymous Access And Authentication של המסך, לחץ על הלחצן Edit. תופיע תיבת הדו-שיח Authentication Methods.

שים לב שגישה Anonymous אינה זמינה לאתר האינטרנט Administration, Basic Authentication אינו מופעל, ו- Integrated Windows Authentication מופעל. משמעות הגדרות אלו היא שדפדפן של לקוח המתחבר לאתר האינטרנט Administration חייב להיות מסוגל לאמת באמצעות Secure NTLM או אימות Kerberos. שיטת אימות Integrated Windows Authentication שתהיה בשימוש תלויה בדפדפן.

14. סמן את תיבת הסימון Digest Authentication For Windows Domain Servers. תופיע תיבת הודעה IIS WWW Configuration, המסבירה שניתן להשתמש רק ב-Windows 2000 Domain Accounts, ושסיסמאות יאוחסנו כטקסט ברור מוצפן.

15. לחץ Yes. פעולה זו מספקת אבטחה נוספת ב-Windows 2000 Domain. תשתמש רק ב-Windows 2000 Domain User Accounts לגישה אל אתר האינטרנט Administration.

16. לחץ OK לסגירת תיבת הדו-שיח Authentication Methods. תופיע תיבת הדו-שיח Administration Web Site Properties.

17. בחלק IP Address And Domain Name Restrictions של המסך, לחץ על הלחצן Edit.

תופיע תיבת הדו-שיח IP Address and Domain Name Restrictions. שים לב שלחצן האפשרות Denied Access נבחר, ושרק הכתובת 127.0.0.1 (שזו הלולאה המקומית, Local Loopback) מקבלת זכאות גישה לאזור זה.

18. לחץ על לחצן האפשרויות Granted Access, כדי שתוכל לגשת לאתר האינטרנט Administration מכל מחשב ברשת התרגול.

לאבטחה נוספת, כדאי לשקול הוספת כתובות IP מפורשות, scope של כתובות IP, או מחשבים בתוך domain מסוים שיוכלו לגשת לאתר האינטרנט Administration. אפשרות זו צורכת משאבים רבים ואינה מומלצת עבור מרבית היישומים של IIS 5.0.

19. לחץ OK.

20. לחץ OK לסגירת תיבת הדו-שיח Administration Web Site Properties. תופיע תיבת הדו-שיח Inheritance Overrides המסבירה שצומת הצאצא, IISAdmin, מגדיר את הערך של Authentication Methods. אתה תדרוס את הערך המוגדר כעת לטובת הערך שהגדרת בצומת Administration Web Site.

21. בתיבה Child Nodes, לחץ על IISAdmin ולחץ OK. תיבת הדו-שיח Inheritance Overrides תופיע שוב עבור צומת הצאצא IISHelp.

22. לחץ על IISHelp ולחץ OK.

23. סגור את תוסף התוכנה Internet Information Services.

הליך 2: גישה לאתר האינטרנט Administration מתוך Internet Service Manager (HTML)

בהליך זה תנסה לגשת לאתר האינטרנט Administration עם ההגדרות החדשות שהגדרת בהליך הקודם.

הערה את המשתנה tcp_port בהליך זה **יש** להחליף בערך שמצאת בהליך הקודם.

---

1. ב- Server01, לחץ Start ולחץ Run. תופיע תיבת הדו-שיח Run.

2. בתיבת הטקסט Open, הקלד **http://server01:<tcp_port>** ולחץ OK.

   Internet Explorer יתחיל, ותופיע תיבת טקסט Microsoft Internet Explorer המסבירה שאינך מפעיל חיבור מאובטח עבור ניהול מבוסס Web.

   פירוש הדבר שבעוד שמידע האימות בין הדפדפן לבין אתר האינטרנט Administration מאובטח, העברת נתונים לאחר הקמת החיבור, אינה מאובטחת.

3. לחץ OK. Internet Explorer יציג את ממשק Internet Services Manager (HTML).

4. חקור את שלושת אתרי האינטרנט המוצגים בחלון העיקרי של הממשק. השתמש בקישורים במסגרת השמאלית לחקר התכונות שנידונו בשיעור זה.

5. סגור את Internet Explorer.

הליך 3: הגדרת גישת SSL לאתר האינטרנט Administration

בהליך זה, תחיל את פרוטוקול SSL על אתר האינטרנט Administration, ליצירת תקשורת מאובטחת בעת פעולה באתר זה. כדי לעשות זאת, תנפיק תעודת שרת תוך שימוש ב- Server01 ו- Certificate Services.

הערה את Certificate Services התקנת בפרק 11, תרגיל 1: "התקנה והגדרה של שירותי אישורים"

---

1. ב-Server01, פתח את Internet Services Manager. יופיע תוסף התוכנה Internet Information Services.
2. בחלון Tree, הרחב את server01 *
3. לחץ על Administration Web site.
4. פתח את תפריט Action, ולחץ על Properties. תופיע תיבת הדו-שיח Administration Web Site Properties.
5. בחר בכרטיסיה Directory Security.
6. באזור Secure Communications של המסך, לחץ על Server Certificate. יופיע אשף Welcome to the Web Server Certificate.
7. קרא את המידע במסך זה ואז לחץ Next. יופיע אשף IIS Certificate.
8. ודא שלחצן האפשרות Create A New Certificate נבחר, ולחץ Next. יופיע מסך Delayed or Immediate Request.
9. לחץ על לחצן האפשרות Send The Request Immediately To An Online Certification Authority, ולחץ Next. יופיע מסך Name and Security Settings.

   שים לב ששם ברירת המחדל הניתן לתעודה זו הוא Administration Web Site ושהאורך בסיביות מוגדר ל- 512 סיביות.
10. לחץ Next. יופיע המסך Organization Information.
11. בתיבת הרשימה הנפתחת Organization, הקלד **Microsoft Corporation**, ובתיבת הרשימה הנפתחת Organizational Unit, הקלד **Microsoft Press**.
12. לחץ Next. יופיע המסך Your Site's Common Name.
13. בתיבת הטקסט Common Name, הקלד **server01.microsoft.com.** ולחץ Next.

    יופיע המסך Geographical Information.
14. אל תשנה את הערך בתיבת הרשימה הנפתחת Country/Region.
15. בתיבת הרשימה הנפתחת State/Province, הקלד **Washington** ובתיבת הרשימה הנפתחת City/Locality, הקלד **Redmond**.

16. לחץ Next. יופיע המסך Choose a Certification Authority, ובתיבת הרשימה הנפתחת Certification Authorities יופיע server01.microsoft.com\Enterprise CA.
17. לחץ Next. יופיע המסך Certificate Request Submission.
18. קרא את מידע התקציר במסך זה, ולחץ Next. לאחר מספר רגעים, יופיע המסך Completing the Web Server Certificate Wizard.
19. לחץ Finish. תופיע תיבת הדו-שיח Administration Web Site Properties. שים לב שתחת אזור Secure Communications של המסך, הלחצנים View Certificate ו-Edit, זמינים עתה.
20. באזור Secure Communications של המסך, לחץ על הלחצן Edit. תופיע תיבת הדו-שיח Secure Communications.
21. סמן את תיבת הסימון Require Secure Channel (SSL).
22. ודא שלחצן האפשרות Ignore Client Certificates נבחר, ולחץ OK. תופיע תיבת הדו-שיח Administration Web Site Properties.
23. בחר בכרטיסיה Web Site.
24. בשדה SSL Port, הקלד **5000**.
25. לחץ OK.
26. סגור את תוסף התוכנה Internet Information Services.

הליך 4: בדיקת גישה לאתר האינטרנט Administration המאובטח

בהליך זה תבדוק את הגישה לאתר האינטרנט Administration, לאחר שהגדרת תעודת שרת ו-SSL עבור האתר.

1. ב-Server01, לחץ Start ולחץ Run. תופיע תיבת הדו-שיח Run.
2. בתיבת הטקסט Open, הקלד **http://server01:<tcp_port>**, ולחץ OK.

   את המשתנה tcp_port בהליך זה יש להחליף בערך שנמצא בהליך 1.

   Internet Explorer יתחיל, ותופיע הודעה המסבירה שיש להציג את הדף על פני ערוץ מאובטח.
3. בתיבת הרשימה הנפתחת Internet Explorer Address, הקלד **https://server01.microsoft.com:5000**, ולחץ Go. הערך 5000 הוא ערך SSL_port שהזנת בכרטיסיה Web Site.

   תופיע תיבת הודעת אבטחה, שבה כתוב שכעת יוצג מידע על פני חיבור מאובטח.
4. סמן את תיבת הסימון In The Future Do Not Show This Warning, ולחץ OK.

   תופיע תיבת הדו-שיח Enter Password.
5. בתיבת הטקסט User Name, הקלד **Administrator**, בתיבת הטקסט Password, הקלד **password**, ובתיבת הטקסט Domain, הקלד **microsoft**.
6. סמן את תיבת הסימון Save This Password In Your Password List, ולחץ OK.

   יוצג הממשק (HTML) Internet Services Manager. שים לב שיש סמל מנעול בפינה הימנית-התחתונה של שורת המצב.
7. הצב את מצביע העכבר מעל סמל המנעול.

   שים לב שמוצג כיתוב "SSL secured (56 bit)". הצפנת 128 סיביות זמינה מתיבת הדו-שיח Secure Communications עבור המאפיינים של האתר. בהליך הקודם, הגדרת SSL עבור החיבור אולם לא קבעת הצפנת 128 סיביות.
8. לחץ לחיצה כפולה על סמל המנעול. תופיע תיבת הדו-שיח Certificate.
9. קרא את המידע בכרטיסיות השונות של תיבת הדו-שיח Certificate. מתיבת הדו-שיח Certificate ניתן להפעיל את אשף Certificate Import להעתקת מידע תעודות מהמחשב המקומי אל מחסן תעודות.
10. לחץ OK.
11. סגור את ממשק (HTML) Internet Services Manager.

סיכום שיעור

IIS 5.0 מציג שיפורים באמינות וביצועים, ניהול, אבטחה וסביבת יישומים. IIS גם מציג תכונות, בהן ניתן להשתמש לשיפור המהירות והביצועים של אתרי אינטרנט, כמו למשל, הוספת הגנה על יישומים באמצעות תמיכה ביישומים במאגר מחוץ-להליך. בנוסף, IIS 5.0 מקל על המנהלים את השימוש בשרת האינטרנט. לדוגמה, הליך ההתקנה מובנה לתוך התקנת Windows 2000 Server. בנוסף, כדי להקל על הגדרת אפשרויות אבטחה, נוספו שלושה אשפי אבטחה. תכונות אבטחה הן נושא חשוב בשיפורים ב-IIS 5.0, המנצל את תכונות האבטחה בעלות תקן-אינטרנט המשולבות לחלוטין ב- Windows 2000. IIS 5.0 גם מוסיף שיפורי ביצועים המקלים על איתור ופתרון בעיות והפעלת יישומי אינטרנט. התקנה והסרה של IIS מבוצעות באחת משלוש דרכים: בעת התקנה או שדרוג Windows 2000, על ידי שימוש ביישומון Add/Remove Programs שבלוח הבקרה, או על ידי שימוש בקובץ unattended.txt, בעת התקנה אוטומטית. כאשר IIS מותקן, נוצרים אתר אינטרנט Default, אתר אינטרנט Administration, ושרת דואר וירטואלי Default SMTP. יש להגדיר את אתרי האינטרנט על ידי ציון איזה ספריות מכילות את המסמכים שרוצים לפרסם. כל אתר אינטרנט או FTP חייב לכלול ספריית בית אחת. כדי לפרסם מספריה כלשהי שאינה כלולה בספריית הבית, ניתן ליצור ספריה וירטואלית. Windows 2000 כוללת את Microsoft ASP, סביבת תסריטי צד-שרת, בה ניתן להשתמש לאוטומציה וריכוזיות של משימות ניהול אתר אינטרנט רבות.

שיעור 2: ניהול סביבת אינטרנט

כאשר מותקן IIS, נוצר אתר אינטרנט ברירת מחדל (Default), המאפשר לממש בקלות ובמהירות סביבת אינטרנט. אולם, ניתן לשנות סביבת אינטרנט זו, כך שתענה על הצרכים המסוימים שלך. בנוסף, ניתן להפעיל WebDAV, המאפשר לשתף מסמכים על פני האינטרנט או רשת אינטראנט. שיעור זה עוסק במספר היבטים של ניהול סביבת אינטרנט: ניהול אתר אינטרנט, ניהול אתר FTP, ופרסום WebDAV. ניהול אתרי אינטרנט ו-FTP דומה מאוד, ולכן שני הנושאים נידונים יחד. לאחר מכן נדון בפרסום WebDAV.

לאחר שיעור זה, תוכל

- לנהל אתרי אינטרנט ו-FTP.
- לנהל פרסום WebDAV.

זמן לימוד משוער: 35 דקות

ניהול אתרי אינטרנט ו-FTP

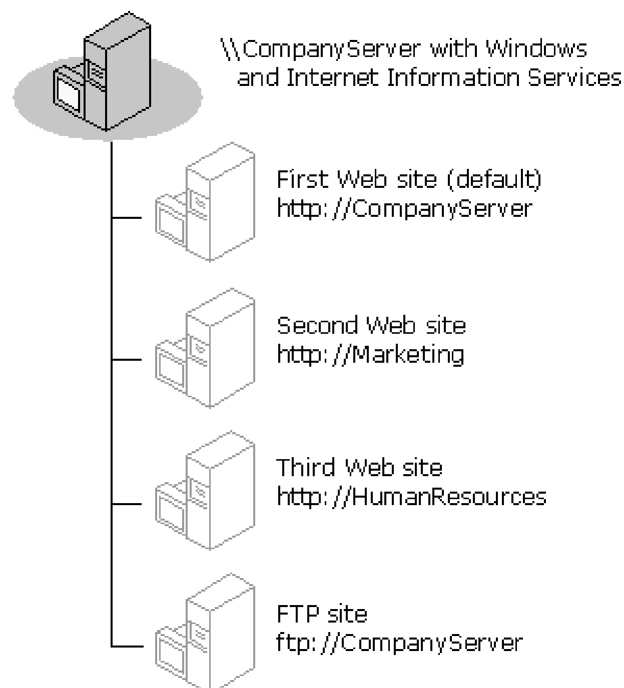
בעבר, כל שם domain, כגון www.microsoft.com, ייצג מחשב יחיד. בעזרת IIS 5.0, ניתן לארח מספר אתרי אינטרנט או אתרי FTP על מחשב יחיד המפעיל Windows 2000 Server. כל אתר אינטרנט יכול לארח שם Domain אחד או יותר. מכיון שכל אתר מחקה את החזות של מחשב יחיד, אתרים מכונים לעיתים **שרתים וירטואליים** (Virtual Servers).

אתרי אינטרנט ואתרי FTP

בין אם המערכת נמצאת ברשת אינטראנט או באינטרנט, ניתן ליצור מספר אתרי אינטרנט ואתרי FTP על מחשב יחיד המפעיל Windows 2000 באחת משלוש דרכים:

- הוספת כתובות יציאה לכתובת IP.
- שימוש במספר כתובות IP, שלכל אחת מהן יש כרטיס מתאם רשת נפרד.
- הקצאת מספר שמות domain וכתובות IP לכרטיס מתאם רשת יחיד, על ידי שימוש בשמות כותרת מארח (Host Header Names).

הדוגמה בתרשים 14.13 מדגימה תרחיש אינטראנט שבו מנהל המערכת התקין את Windows 2000 Server עם IIS על שרת של חברה, ויצר אתר אינטרנט ברירת מחדל יחיד: http://CompanyServer. אז, יצר מנהל המערכת שני אתרי אינטרנט נוספים, אחד עבור כל אחת משתי מחלקות: שיווק ומשאבי אנוש.



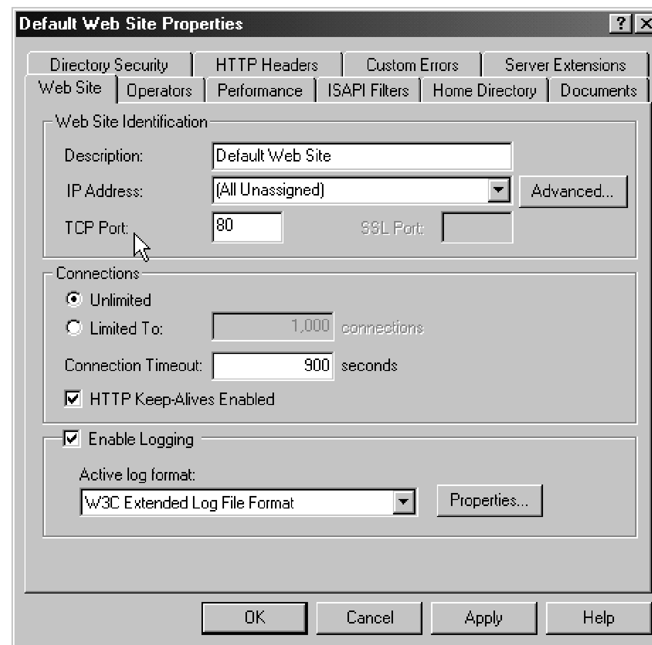
תרשים 14.13 אינטראנט עם מספר אתרי אינטרנט.

למרות שהם מתארחים על מחשב יחיד, CompanyServer, Marketing, ו-HumanResources נראים כל אחד, כאילו הוא אתר אינטרנט נפרד. אתרים מחלקתיים אלה נהנים מאותן אפשרויות אבטחה שהיו להם, אילו הם היו קיימים על מחשבים נפרדים, כיון שלכל אתר יש הגדרות הרשאה, ניהול וגישה שונות. בנוסף, ניתן להעביר את המשימות הניהוליות לחברים בכל מחלקה.

הערה בעת יצירת מספר גדול מאוד של אתרים, יש להקפיד ולהתייחס למגבלות רשת וחומרת מחשב, ולשדרג משאבים אלה כנדרש.

מאפיינים וירושת מאפיינים באתרים

מאפיינים (Properties) הם ערכים שניתן להגדיר באתר האינטרנט. לדוגמה, ניתן להשתמש בתוסף התוכנה Internet Information Services, לשינוי יציאת TCP המוקצית לאתר האינטרנט כברירת המחדל, מערך ברירת המחדל 80 למספר יציאה אחר. מאפיינים של אתר יחיד מוצגים בתיבת הדו-שיח Properties (תרשים 14.4) עבור אתר זה ומאוחסנים במסד נתונים הנקרא Metabase.



תרשים 14.14 תיבת הדו-שיח Properties עבור אתר אינטרנט Default.

בעת התקנת IIS, הוקצו ערכי ברירת מחדל למאפיינים השונים. ניתן להשתמש בערכי ברירת המחדל ב- IIS, או להתאים אישית את ההגדרות, כך שיתאימו לצרכי הפרסום באינטרנט. ייתכן שניתן יהיה לספק ערך מוסף, ביצועים טובים יותר, ושיפור באבטחה על ידי שינוי הגדרות ברירת המחדל.

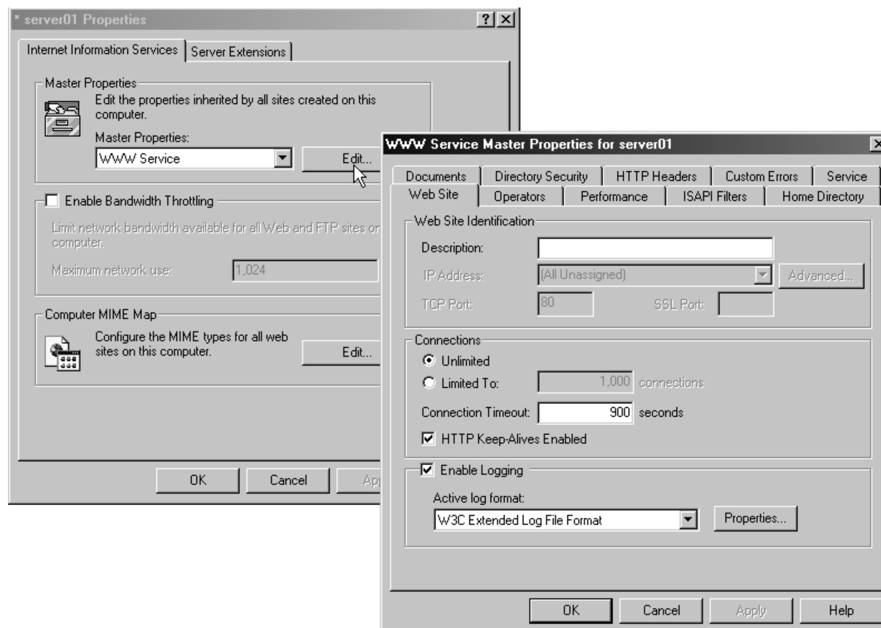
הערה בתרגיל 1 בפרק זה שינית את מאפייניו של אתר האינטרנט Administration להגברת האבטחה של אזור רגיש זה.

ניתן להגדיר מאפיינים ברמת האתר, ברמת הספריה, או ברמת הקובץ. הגדרות ברמות גבוהות יותר (כגון ברמת האתר) משמשות אוטומטית, או עוברות בירושה, אל הרמות הנמוכות יותר (כמו רמת הספריה). אולם, עדיין ניתן לערוך אותן ידנית גם ברמה הנמוכה יותר. לאחר שמאפיין השתנה באתר, ספריה, או קובץ מסוימים, שינויים מאוחרים יותר בברירות המחדל הראשיות לא ידרסו אוטומטית את ההגדרה הנפרדת.

במקום זאת, תתקבל הודעת אזהרה ובה שאלה, האם רוצים לשנות את הגדרות האתר, הספריה, או הקובץ הבודדים, כך שיתאימו לברירת המחדל החדשה.

לחלק מהמאפיינים יש ערך בצורת רשימה. לדוגמה, ערך מסמך ברירת המחדל יכול להיות רשימת מסמכים אותם יש לטעון כאשר משתמשים אינם מציינים שם קובץ בכתובת ה-URL. הודעות שגיאה מותאמות אישית, בקרת גישת TCP/IP, מיפויי תסריטים, ומיפויי MIME הן דוגמאות נוספות למאפיינים המאוחסנים בצורת רשימה. למרות שברשימות אלו יש מספר ערכים, IIS מתייחס לרשימה כולה כאל מאפיין יחיד. אם עורכים רשימה בספריה ואז מבצעים שינוי גלובלי ברמת האתר, הרשימה ברמת הספריה מוחלפת לחלוטין ברשימה החדשה מרמת האתר, הרשימות אינן ממוזגות. בנוסף, מאפיינים עם ערכים בצורת רשימה מציגים את הרשימות שלהם ברמה העיקרית בלבד, או באתר או בספריה אשר השתנו ביחס לערך ברירת המחדל. ערכי רשימה אינם מוצגים אם הם ברירת המחדל שעברה בירושה.

מאפיינים עיקריים, הרחבות שרת, Bandwidth throttling, ומיפוי MIME עבור השירותים של אתר מוצגים מהמאפיינים של צומת מחשב, המופיע בתוסף התוכנה Internet Information Services או בממשק (HTML) Internet Services Manager. תרשים 14.15 מציג את המאפיינים העיקריים של WWW Service, שהגישה אליהם בוצעה בעזרת הלחצן Edit במסך Properties של צומת מחשב.



תרשים 14.15 WWW Service Master Properties עבור Server01.

בממשק Internet Services Manager (HTML) קיים קישור Master Properties ותיבת הרשימה הנפתחת במסגרת השמאלית של דף הבית (תרשים 14.2).

מסנני **I**nternet **S**erver API (ISAPI) מוצגים בתצורת רשימה, אולם אינם זוכים ליחס של רשימה. אם מוסיפים מסננים ברמת האתר, המסננים החדשים ממוזגים עם רשימת המסננים של הרמה העיקרית. אם שני מסננים מוגדרים ברמת עדיפות זהה, המסנן מהרמה העיקרית נטען לפני המסנן מרמת האתר. מסנני ISAPI המותקנים, והעדיפות שלהם מוצגים מתוך הכרטיסיה ISAPI Filters שב- WWW Service Master Properties, ובדף המאפיינים של כל אתר אינטרנט.

אם יש צורך לשנות את ערכי ברירת המחדל של מאפיינים, ויוצרים מספר אתרי אינטרנט או FTP, ניתן לערוך את ערכי ברירת המחדל, כך שכל אתר שיוצרים יירש את הערכים המותאמים אישית.

הקבוצה Operators

מפעילים (Operators) הם קבוצת משתמשים מיוחדת בעלת זכויות ניהול מוגבלות באתרי אינטרנט מסוימים. חברים בקבוצה Operators יכולים לנהל מאפיינים המשפיעים על האתרים המסוימים שלהם בלבד. אין להם גישה למאפיינים המשפיעים על IIS, על שרת Windows המארח את IIS, או על הרשת.

לדוגמה, ספק שירותי אינטרנט, המארח אתרים עבור מספר חברות שונות, יכול להקצות נציגים מכל חברה כמפעילים עבור אתר האינטרנט של החברה. שיטה זו של ניהול שרת מבוזר מספקת את היתרונות הבאים:

- כל חבר בקבוצה Operators יכול לפעול כמנהל האתר ויכול לשנות או להגדיר מחדש את אתר האינטרנט לפי הצורך. לדוגמה, המפעיל יכול להגדיר הרשאות באתר האינטרנט, לאפשר רישום יומנים, לשנות את מסמך ברירת המחדל או הכותרת התחתונה, להגדיר תפוגת תוכן ולאפשר תכונות דירוג תוכן.
- מפעיל אתר האינטרנט אינו רשאי לשנות את הזיהוי של אתרי אינטרנט, להגדיר שם וסיסמה עבור משתמש אנונימי, מצערת (Throttle) רוחב פס, ליצור ספריות וירטואליות, או לשנות את הנתיבים שלהן, או לשנות בידוד יישומים.
- כיון שחברים בקבוצה Operators מקבלים זכויות מוגבלות יותר מאלו של מנהלי אתרי אינטרנט, הם אינם יכולים לעיין מרחוק במערכת הקבצים, ולכן אינם יכולים להגדיר מאפיינים עבור ספריות וקבצים, אלא אם משתמשים בנתיב UNC.

ניהול אתרים מרחוק

מכיון שלא תמיד נוח לבצע משימות ניהול על המחשב המפעיל את IIS, קיימות שתי אפשרויות לניהול מרחוק. אם מתחברים אל השרת על פני האינטרנט או דרך שרת Proxy, ניתן להשתמש ב- Internet Services Manager (HTML) המבוסס על דפדפן לשינוי מאפיינים באתר. אם החיבור הוא באינטראנט, ניתן להשתמש ב- Internet Services Manager (HTML) או בתוסף התוכנה Internet Information Services. למרות ש- Internet Services Manager (HTML) מציע רבות מהתכונות הקיימות בתוסף התוכנה, שינויי מאפיינים הדורשים תיאום עם תוכניות שירות של Windows, כגון מיפוי תעודות, לא ניתנים לביצוע עם Internet Services Manager (HTML).

הערה בגרסאות הקודמות תוסף התוכנה Internet Information Services נקרא Internet Services Manager. **תוסף התוכנה** Internet Information Services **מופיע בתפריט** Administrative Tools **כ-** Internet Services Manager.

Internet Services Manager (HTML) משתמש באתר אינטרנט הרשום כאתר Administration לגישה אל מאפייני IIS. כאשר מתקינים IIS, מספר יציאה בין 2,000 ל- 9,999 נבחר באופן אקראי ומוקצה לאתר אינטרנט זה. האתר מגיב לבקשות דפדפן עבור כל שמות ה-Domain המותקנים במחשב, בתנאי שמוסיפים את מספר היציאה בסוף הכתובת. אם משתמשים באימות בסיסי (Basic Authentication), המנהל יתבקש לספק שם משתמש וסיסמה כאשר הוא מגיע לאתר. רק חברים בקבוצה Administrators ובקבוצה Operators יכולים להשתמש באתר.

הערה למרות שגרסת HTML של Internet Services Manager (HTML) **דומה מאוד** בפונקציונליות שלה לתוסף התוכנה Internet Information Services, גרסת HTML מתוכננת כדף אינטרנט. אין תמיכה בגישה לתפריטי קיצור או לאובייקטי ממשק. רבים מלחצני סרגל הכלים או כותרות הכרטיסיות המוכרים מוצגים כקישורים במסגרת השמאלית. בשל הבדלים אלה, ייתכן שההוראות בתיעוד אינן תואמות בדיוק את השלבים המבוצעים ב-Internet Services Manager (HTML).

ניתן גם להשתמש ב- Terminal Services על פני חיבור רשת (כגון LAN, PPTP או חיבור בחיוג) לניהול IIS מרחוק. Terminal Services אינו דורש התקנה של **M**icrosoft **M**anagement **C**onsole (MMC) או את תוסף התוכנה Internet Information Services על המחשב המרוחק.

התיעוד המקוון של IIS 5.0 זמין לשימוש כאשר מבצעים משימות ניהול מרחוק. כדי להגיע לתיעוד, הפעל את אתר האינטרנט Administration, ואז לחץ על סמל הספר בפינה הימנית-העליונה של דף הבית. קישור זה פותח חלון חדש ל-URL הבא: http://<servername>/iishelp/iis/misc/default.asp, כאשר <servername> הוא שם מזהה (כתובת IP, שם מחשב, או FQDN) של המחשב המפעיל IIS.

פונקציית החיפוש של תיעוד IIS תלויה ב- Indexing Service המותקן ב- Windows 2000 Server כברירת מחדל אולם מוגדרת להפעלה ידנית. Indexing Service מוגדר מתוך תוסף התוכנה Computer Management תחת הצומת Services and Applications. כדי שתיעוד IIS 5.0 יסומן באינדקסים לחיפוש, הוסף את הנתיב הפיסי לתיקיה iisHelp אל הספריה Web Directories עבור Indexing Service. לאחר הגדרת Indexing Service, ניתן להעביר את ההפעלה למצב אוטומטי באמצעות תוסף התוכנה Services.

הערה Indexing Service עשוי לדרוש הרבה פעולות מעבד, במיוחד אם יש לבצע אינדקסים של חומר רב. כדאי להפעיל פונקציות Indexing Service על מחשב הכולל מספיק משאבים לאפשור פעולות אלו.

FTP Restart

FTP Restart מתייחס לבעיה של אובדן חיבור רשת בעת הורדת קבצים. לקוחות התומכים ב- FTP Restart צריכים רק ליצור מחדש את חיבור FTP, והעברת הקבצים ממשיכה אוטומטית מהמקום בו היא נפסקה.

הערה יישום IIS 5.0 של FTP Restart אינו מופעל כאשר משתמשים ב-FTP להורדת בקשות תווים כלליים (MGET), העלאת קבצים לשרת (PUT), או הורדת קבצים הגדולים מ- 4GB.

ניהול אתרים

הליך ניהול אתרים כולל מספר משימות, כגון הפעלה והפסקת אתרים, הוספת אתרים, מתן שמות לאתרים והפעלה מחדש של IIS.

הפעלה והפסקת אתרים

כברירת מחדל, אתרים מתחילים אוטומטית, כאשר המחשב מתחיל מחדש. הפסקת אתר מפסיקה שירותי אינטרנט, ומורידה אותם מזיכרון המחשב. עצירה זמנית (Pausing) של אתר מונעת משירותי אינטרנט לקבל חיבורים חדשים, אך אינה משפיעה על בקשות שכבר נמצאות בשלבי עיבוד. הפעלת אתר מפעילה מחדש או ממשיכה את שירותי אינטרנט.

כדי להפעיל, להפסיק, או לעצור זמנית אתר, השתמש בתוסף התוכנה Internet Information Services. בחר את האתר הרצוי להפעלה, הפסקה או עצירה זמנית, ואז לחץ על לחצן Start Item, Stop Item, או Pause Item בהתאמה בסרגל הכלים.

הערה אם אתר מפסיק באופן לא צפוי, תוסף התוכנה Internet Information Services עלול לציין בצורה שגויה את מצב השרת. לפני הפעלה מחדש, לחץ על Stop, ואז לחץ על Start להפעלת האתר מחדש.

הוספת אתרים

ניתן להוסיף אתרים חדשים למחשב על ידי הפעלת אשף Web Site Creation, אשף FTP Site Creation, או אשף SMTP Virtual Server בתוסף התוכנה Internet Information Services. בחר את המחשב או האתר, פתח את תפריט Action, לחץ על New, ואז לחץ על Web Site, FTP Site או SMTP Virtual Server להפעלת האשף המתאים.

הערה אשף SMTP Virtual Server **הוא מחוץ להיקף ספר זה, ולכן אינו מוסבר בפירוט.**

מלא אחר ההוראות על המסך להקצאת מידע זיהוי לאתר החדש. יש לציין את כתובת היציאה ואת נתיב ספריית הבית. אם מוסיפים אתרים נוספים לכתובת IP יחידה, על ידי שימוש בכותרות מארח, יש להקצות שם כותרת מארח.

הערה **האפשרות** All Unassigned **(הכל לא מוקצה) ברשימה הנפתחת** Enter the IP address to use for this Web Site **שבאשף** Web Site Creation **(או ברשימה הנפתחת** IP Address **באשף** FTP Site Creation**) מתייחסת לכתובות** IP **המוקצות למחשב, אך אינן מוקצות לאתר מסוים. אתר האינטרנט ברירת המחדל משתמש בכל כתובות** IP **שאינן מוקצות לאתרים אחרים. ניתן להגדיר רק אתר אחד לשימוש בכתובות** IP **שאינן מוקצות.**

מתן שמות לאתרי אינטרנט

לכל אתר אינטרנט (שרת וירטואלי) יש שם תיאורי והוא יכול לתמוך בשם כותרת מארח אחד או יותר. שמות כותרת מארח (Host Header Name) מאפשרים לארח מספר שמות domain על מחשב יחיד. לא כל הדפדפנים תומכים בשימוש בשמות כותרת מארח. Internet Explorer 3.0, Netscape Navigator 2.0, וגרסאות מאוחרות יותר של שני הדפדפנים תומכות בשימוש בשמות כותרת מארח, גרסאות קודמות שלהם אינן תומכות בכך.

אם אורח מנסה להתחבר לאתר עם דפדפן מיושן, שאינו תומך בכותרות מארח, הוא מופנה לאתר אינטרנט ברירת המחדל המוגדר לכתובת IP זו (אם מופעל אתר ברירת מחדל), ולא בהכרח לאתר המבוקש. בנוסף, אם בקשה מדפדפן כלשהו מתקבלת עבור אתר שנעצר, האורח מקבל במקומו את אתר ברירת המחדל. לכן, כדאי לשקול בזהירות מה מציג אתר ברירת המחדל. בדרך כלל, ספקי שירותי אינטרנט מציגים את דף הבית שלהם כברירת המחדל, ולא אתר של אחד מלקוחותיהם. הדבר מונע מבקשות עבור אתר שנעצר להגיע לאתר הלא-נכון. בנוסף, אתר ברירת המחדל יכול לכלול תסריט שתומך בשימוש בשמות כותרת מארח עבור דפדפנים מיושנים.

ניתן להשתמש בתוסף התוכנה Internet Information Services למתן שם לאתר. בחר אתר אינטרנט, ופתח את תיבת הדו-שיח Properties שלו. בכרטיסיה Web Site, הקלד שם תיאורי עבור האתר בתיבה Description (תרשים 14.14).

הפסקה, התחלה, התחלה מחדש, או אתחול ב- IIS

ב- IIS 5.0, ניתן להפסיק, להתחיל, או לאפס (אפשרות התחלה מחדש) את כל שירותי האינטרנט או לאתחל את השרת מתוך תוסף התוכנה Internet Information Services. הפעולות הפסקה, התחלה או התחלה מחדש מפחיתות את הסיכויים שיהיה צורך לאתחל מחדש את השרת, כאשר יישומים אינם פועלים כנדרש או שאינם זמינים.

הפעולה התחל מחדש (Restart) מפסיקה ומתחילה בצורה נוחה שירותי אינטרנט, תוך איפוס יעיל של השירות. כדי להתחיל מחדש את IIS, בחר את צומת המחשב בחלון Tree, פתח את תפריט Action, ואז לחץ על Restart IIS. תרשים 14.16 מציג את תיבת הדו-שיח Stop/Start/Reboot המופיעה.



תרשים 14.16 התחלה מחדש של שירותי אינטרנט על Server01.

תיבת הרשימה הנפתחת המוצגת בתרשים 14.16 מכילה גם אפשרויות התחל והפסק של IIS, ואת האפשרות Reboot Server.

חשוב התחלה מחדש תעצור את כל תהליכי Drwtsn32.exe, Mtx.exe, ו-Dllhost.exe כדי להתחיל מחדש את שירותי אינטרנט. לא ניתן להפסיק או להתחיל את IIS, או לאתחל מחדש את השרת באמצעות (HTML) Internet Services Manager המבוסס על הדפדפן. אולם ניתן להשתמש הן בתוסף התוכנה והן בממשק HTML להפסקה, התחלה, עצירה זמנית והתחלה מחדש של אתרים בודדים.

יש להשתמש בתוסף התוכנה Internet Information Services להתחלה מחדש של שירותי אינטרנט, ולא בתוסף התוכנה Services ב-Computer Management. מכיון שמספר שירותי אינטרנט פועלים בהליך יחיד, שירותי אינטרנט מופסקים ומתחילים מחדש באופן שונה מאשר שירותי Windows אחרים.

גיבוי ושחזור IIS

ניתן לגבות את הגדרות תצורת IIS, כך שיהיה קל לחזור למצב קודם. השלבים לשחזור תצורה יהיו שונים אם הסרת והתקנת מחדש את IIS או לא.

ניתן להשתמש בתוסף התוכנה Internet Information Services לגיבוי תצורת IIS. בחר את צומת Computer בחלון Tree, פתח את תפריט Action, ובחר Backup/Restore Configuration.

שיטת גיבוי זו תספק דרך לשחזור הגדרות IIS בלבד, ולא את קבצי התוכן. בנוסף, שיטה זו לא תפעל אם תתקין מחדש את מערכת ההפעלה, וקבצי הגיבוי אינם יכולים לשמש לשחזור הגדרת IIS על מחשבי Windows 2000 אחרים.

הערה ניתן לגבות את IIS באמצעות ממשק Internet Services Manager (HTML), אולם חייבים להשתמש בתוסף התוכנה Internet Information Services לשחזור הגדרות התצורה. הקישור Backup Configuration מופיע בחלונית השמאלית של ממשק Internet Services Manager (HTML), (תרשים 14.2).

לשחזור הגדרות תצורת IIS בתוסף התוכנה Internet Information Services, בחר את הצומת Computer בחלון Tree, פתח את תפריט Action, ולחץ על Backup/Restore Configuration. בחר קובץ גיבוי, ולחץ על הלחצן Restore. כאשר תוצג שאלה האם לשחזר את הגדרות התצורה, לחץ Yes.

ניהול פרסום WebDAV

WebDAV מרחיב את פרוטוקול HTTP/1.1, כדי לאפשר ללקוחות לפרסם, לנעול ולנהל משאבים באינטרנט. WebDAV, המשולב לתוך IIS, מאפשר ללקוחות לבצע את הפעולות הבאות:

- לטפל במשאבים בספריית הפרסום WebDAV על השרת. לדוגמה, בעזרת תכונה זו, משתמשים עם ההרשאות המתאימות יכולים להעתיק ולהעביר קבצים ממקום למקום בספריה WebDAV.
- לשנות מאפיינים הקשורים למשאבים מסוימים. לדוגמה, משתמש יכול לכתוב אל ולאחזר מידע מאפיינים של קובץ.

- לנעול ולפתוח משאבים, כך שמספר משתמשים יוכלו לקרוא קובץ בו-זמנית, אולם רק משתמש אחד בכל פעם יוכל לשנות את הקובץ.
- לחפש בתוכן ובמאפיינים של קבצים בספריה WebDAV.

הגדרת ספריית הפרסום WebDAV על השרת פשוטה כמו הגדרת ספריה וירטואלית. לאחר הגדרת ספריית הפרסום, משתמשים בעלי ההרשאות המתאימות יכולים לפרסם מסמכים לשרת, ולטפל בקבצים בספריה זו.

לקוחות WebDAV

ניתן לגשת לספריית הפרסום WebDAV באמצעות אחד ממוצרי Microsoft המתוארים ברשימה הבאה, או דרך לקוח אחר כלשהו התומך בפרוטוקול WebDAV התקני.

- Windows 2000 מתחברת לשרת WebDAV באמצעות אשף Add Network Place, ומציגה את התוכן של הספריה WebDAV כאילו היה חלק מאותה מערכת קבצים על המחשב המקומי. לאחר החיבור, ניתן לגרור ולשחרר קבצים, לאחזר ולשנות מאפייני קבצים, ולבצע משימות מערכת קבצים רבות אחרות.

  לדוגמה, אם יוצרים ספריה וירטואלית בשם WebDAV תחת אתר האינטרנט Default על server01.microsoft.com, ניתן לגשת אליה מהכתובת הבאה: http://server01.microsoft.com/webdav/.

- Internet Explorer 5 מתחבר לספריה WebDAV, ומאפשר לבצע את אותן משימות מערכת קבצים שניתן לבצע דרך Windows 2000.

  הקפד להפעיל את הרשאת Directory Browsing במאפיינים של ספריה וירטואלית, כדי לגשת לספריה הוירטואלית באמצעות Internet Explorer 5.

- Office 2000 יוצרת, מפרסמת, עורכת ושומרת מסמכים ישירות לתוך הספריה WebDAV דרך כל יישום ב- Office 2000.

חיפוש ב-WebDAV

לאחר התחברות לספריה WebDAV, ניתן לחפש במהירות בין הקבצים בספריה זו, לאיתור תוכן בנוסף למאפיינים. לדוגמה, ניתן לחפש את כל הקבצים המכילים את המילה table או את כל הקבצים שנכתבו על ידי Fred.

אבטחה משולבת

מכיון ש-WebDAV משולבת עם Windows 2000 ו- IIS 5.0, היא שואלת את תכונות האבטחה המוצעות על ידי שניהם. תכונות אלו כוללות את הרשאות IIS המוגדרות בתוסף התוכנה Internet Information Services, ואת רשימות הגישה DACL (**D**iscretionary **A**ccess **C**ontrol **L**ist) במערכת הקבצים NTFS.

מאחר שלקוחות עם הרשאות מתאימות יכולים לכתוב לספריה WebDAV, חיוני לשלוט על בעלי הגישה לספריה בכל עת. כדי לסייע בבקרת גישה, IIS 5.0 מחזק את אימות Integrated Windows על ידי הכנסת תמיכה בפרוטוקול האימות Kerberos 5. על ידי בחירת אימות Integrated Windows, ניתן לוודא שרק לקוחות בעלי הרשאה יוכלו לגשת ולכתוב בספריה WebDAV על האינטראנט.

בנוסף, IIS 5.0 מציגה סוג חדש של אימות הנקרא Digest Authentication. סוג אימות זה, שנוצר עבור Windows domain servers, מציע אבטחה הדוקה יותר עבור סיסמאות ועבור העברת נתונים על פני האינטרנט.

יצירת ספריית פרסום

כדי להקים ספריית פרסום (Publishing Directory), צור ספריה פיסית תחת Inetpub. לדוגמה, אם שם הספריה יהיה WebDAV, הנתיב לספריה זו יכול להיות C:\Inetpub\WebDAV.

למעשה, ניתן להציב את הספריה בכל מקום, מלבד תחת הספריה Wwwroot (Wwwroot יוצאת דופן כיון ש-DACLs ברירת המחדל שלה שונים מאלה של ספריות אחרות).

בתוסף התוכנה Internet Information Services, צור אתר אינטרנט חדש, או השתמש באתר קיים, וצור תחתיו ספריה וירטואלית. הקלד **WebDAV**, או שם נוח אחר כלשהו, ככינוי עבור ספריה וירטואלית זו, וקשר אותה אל הספריה הפיסית שיצרת זה עתה. הענק הרשאות קריאה (Read), כתיבה (Write) ועיון (Browse) עבור הספריה הווירטואלית.

אתה מעניק למשתמשים את הזכות לפרסם מסמכים בספריה וירטואלית זו ולראות רשימה של הקבצים בה. למרות שהדבר אינו מומלץ משיקולי אבטחה, ניתן להקצות אותן זכויות גישה לכל אתר האינטרנט, ולאפשר ללקוחות לפרסם בכל שרת האינטרנט.

הערה הענקת גישה לכתיבה אינה מאפשרת ללקוחות לשנות ASP (**A**ctive **S**erver **P**ages) או קבצים ממופי-תסריט אחרים כלשהם. כדי לאפשר שינוי קבצים אלה, יש להעניק זכויות כתיבה וגישה למקור תסריט לאחר יצירת הספריה הוירטואלית.

לאחר סיום הגדרת הספריה WebDAV וירטואלית, ניתן לאפשר ללקוחות לפרסם בה.

ניהול אבטחת WebDAV

כדי להגן על השרת ותוכנות, יש לתאם בין שלושה היבטים שונים של אבטחה ליצירת שלם משולב: אימות לקוחות, בקרת גישה ודחיית שירות.

אימות לקוחות

IIS 5.0 מציע אימות ברמות הבאות:

- **Anonymous** – גישה אנונימית מאפשרת לכל אחד גישה אל הספריה, ולכן, יש לכבות אפשרות זו עבור הספריה WebDAV. בלי שליטה על בעלי הגישה, ייתכן נזק לספריה מצד לקוחות לא ידועים.
- **Basic** – אימות בסיסי שולח סיסמאות על פני החיבור בטקסט ברור. כיון שטקסט ברור חשוף לקליטה וקריאה על ידי האזנה לחיבור, כדאי להפעיל אימות בסיסי רק אם הנתונים מוצפנים באמצעות SSL.
- **Integrated Windows** – אימות Integrated Windows הוא פתרון טוב מאוד, כאשר מגדירים את הספריה WebDAV ברשת אינטראנט.
- **Digest** – אימות Digest הוא הבחירה הטובה ביותר עבור פרסום מידע על שרת על פני האינטרנט ודרך קירות המגן.

ההגדרה הטובה ביותר עבור הספריה WebDAV תלויה בסוג הפרסום שרוצים לבצע. כאשר יוצרים ספריה וירטואלית דרך IIS 5.0, אימות אנונימי ואימות Integrated Windows מופעלים שניהם. למרות שההגדרה של ברירת מחדל זו פועלת היטב עבור לקוחות המתחברים לשרת, קוראים תוכן בדף אינטרנט, ומפעילים תסריטים, היא אינה מתאימה ללקוחות המפרסמים בספריה ומטפלים בקבצים בספריה זו.

בקרת גישה

ניתן לשלוט על הגישה לספריה WebDAV על ידי תיאום הרשאות IIS 5.0 ו- Windows 2000.

הגדרת הרשאות אינטרנט

אופן הגדרת הרשאות אינטרנט מבוסס על מטרת החומר המפורסם.

- **Read, Write, Directory Browsing enabled** – הפעלת הרשאות אלו מאפשרת ללקוחות לראות רשימת משאבים, לשנות אותם (מלבד אותם משאבים ללא הרשאת כתיבה), לפרסם את המשאבים שלהם, ולטפל בקבצים.
- **Write enabled, Read and Directory Browsing disabled** – אם רוצים שלקוחות יפרסמו מידע פרטי בספריה, אך לא רוצים שאחרים יראו מה פורסם, יש להגדיר הרשאת כתיבה, אך לא לאפשר הרשאת קריאה ועיון בספריה. תצורה זו מתאימה למקרים בהם לקוחות מצביעים או מגישים סקירות ביצועים. שים לב שביטול הרשאת Directory Browsing מונעת גישה מדפדפנים ללקוחות המנסים לגשת לספריה WebDAV.

- ❖ **Read and Write enabled, Directory Browsing disabled** – תצורה זו מתאימה כאשר רוצים לסמוך על טשטוש שמות קבצים כאמצעי אבטחה. אולם, יש לזכור כי "אבטחה על בסיס הסתרה" היא שיטה ברמה נמוכה, מכיון שאדם שרוצה לגרום נזק יכול בקלות לנחש שמות קבצים על ידי ניסוי ותעיה.
- ❖ **Index This Resource enabled** – הקפד להפעיל Indexing Service, אם בכוונתך לאפשר ללקוחות לחפש משאבי ספריה.

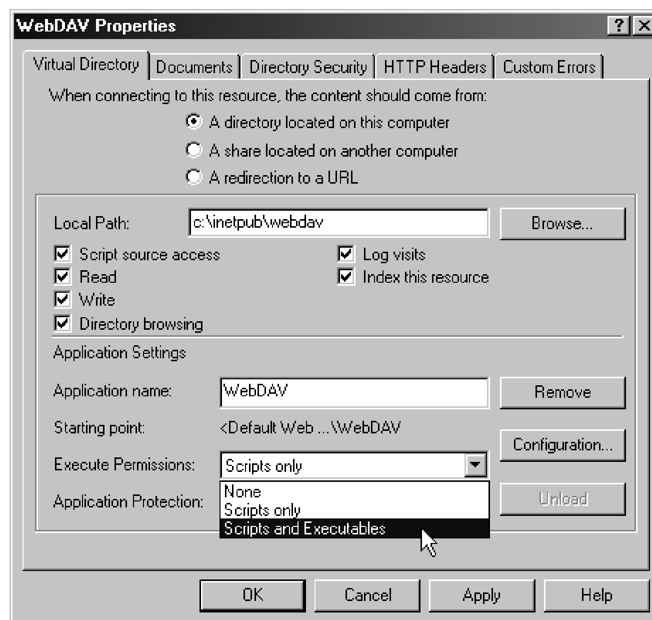
בקרת גישה עם DACLs

בעת הגדרת ספריית פרסום WebDAV על כונן מערכת קבצים NTFS, Windows 2000 נותנת לכולם שליטה מלאה (Full Control) כברירת מחדל. שנה רמת הרשאות זו, כך שלכולם תהיה הרשאת קריאה בלבד. עתה הענק הרשאת כתיבה לבודדים או לקבוצות מסוימות.

הגנה על קוד תסריט

אם בספריית הפרסום קיימים קבצי תסריט שאינך רוצה לחשוף בפני לקוחות, ניתן בקלות למנוע גישה לקבצים אלה על ידי בדיקה שהרשאת גישה למקור תסריט אינה מופעלת. תסריטים כוללים קבצים עם סיומות המוצגות ברשימה Applications Mapping. קבצים ברי-הפעלה אחרים יטופלו כקבצי HTML סטטיים, כולל קבצים עם סיומות exe, אלא אם הופעלה האפשרות Scripts and Executables עבור הספריה.

כדי למנוע הורדת קבצי exe והתייחסות אליהם כאילו הם קבצי HTML, בחר את האפשרות Scripts and Executables מהרשימה הנפתחת Execute Permissions, הממוקמת בכרטיסיה Virtual Directory של תיבת הדו-שיח Properties של ספריית הפרסום (תרשים 14.17).



תרשים 14.17 בחירת האפשרות Scripts and Executables מתוך תיבת הרשימה הנפתחת Execute Permissions

רמת הרשאה זו חושפת את כל הקבצים הניתנים להפעלה להגדרות הגישה של מקור תסריט. במילים אחרות, אם נבחרת גישת מקור תסריט, לקוחות עם הרשאת קריאה יכולים לראות את כל קבצי ההפעלה, ולקוחות עם הרשאת כתיבה יכולים גם לערוך אותם וגם להפעיל אותם. הגדרה זו מהווה סיכון אבטחה, כיון שאז ניתן לפרסם תוכניות בספריה, ולהפעיל אותן לגרימת נזק לאתר.

בעזרת ההרשאות הבאות, לקוחות יכולים לכתוב לקובץ הפעלה שאינו מוצג במיפוי היישום (Application Mapping) :

- הרשאת כתיבה (Write).
- Execute Permissions מוגדר ל- Scripts only.

בעזרת ההרשאות הבאות, לקוחות יכולים גם לכתוב לקובץ הפעלה :

- מתן גישה למקור תסריט.
- Execute Permissions מוגדר ל- Scripts and Executables.

מניעת שירות

גרירה ושחרור קבצים גדולים מאוד לתוך הספריה WebDAV עשויה לצרוך כמות גדולה מאוד של מקום בדיסק. להגבלת כמות זו, כדאי לשקול הגדרת מכסות לשימוש בדיסק.

פרסום וניהול קבצים

משתמשים יכולים להתחבר לספריית פרסום WebDAV, לפרסם מסמכים על ידי גרירתם מהמחשבים שלהם לספריית הפרסום, ולטפל בקבצים בספריה.

הערה גם אם משתמשים מתחברים מעבר לקיר המגן (Firewall), הם **עדיין יכולים** לפרסם בספריה WebDAV, אם **יש** להם **הרשאות מתאימות ואם** קיר מגן זה מוגדר לאפשור פרסום.

ממחשב Windows 2000, ניתן להתחבר לספריית פרסום WebDAV על שרת אחר באמצעות My Network Places.

ניתן גם להתחבר לספריה WebDAV באמצעות Internet Explorer 5 על מערכות ההפעלה Windows 2000, Windows NT 4.0, Windows 98 או Windows 95. לאחר החיבור, ניתן לטפל בקבצים ולפרסם לספריה זו, בדיוק כפי שניתן היה לאחר התחברות דרך Windows 2000. בנוסף, ניתן ליצור, לפרסם, או לשמור מסמכים בספריה WebDAV דרך כל יישום Office 2000.

סיכום שיעור

ניתן לארח מספר אתרי אינטרנט או FTP בו-זמנית על מחשב יחיד המפעיל Windows 2000 Server. הדבר נראה כמו מספר מחשבים. כל אתר אינטרנט יכול לארח שם domain אחד או יותר. הליך ניהול האתרים כולל מספר משימות, כגון הפעלה והפסקה של אתרים, הוספת אתרים, מתן שמות לאתרים והפעלה מחדש של IIS. ניתן לגבות את תצורת IIS, כך שיהיה קל לחזור למצב קודם, וניתן לנהל את IIS מרחוק. WebDAV מרחיב את פרוטוקול HTTP/1.1 ומאפשר ללקוחות לפרסם, לנעול ולנהל משאבים באינטרנט. לאחר התחברות לספריה WebDAV, ניתן במהירות לחפש בין הקבצים בספריה זו לאיתור תוכן, בנוסף למאפיינים. ניתן להציב ספריית WebDAV בכל מקום שרוצים, מלבד תחת הספריה Wwwroot. ניתן להגן על השרת והתוכן על ידי תיאום ושילוב היבטים שונים של אבטחה (אימות לקוחות, בקרת גישה, ומניעת שירות). לאחר יצירת הספריה WebDAV לפרסום, ניתן להגדיר את הספריה כך שתאפשר למשתמשים לחפש תוכן ומאפייני קבצים. מ- Windows 2000 ניתן להתחבר לספריית פרסום WebDAV על שרת אחר. ניתן להתחבר לספריית WebDAV דרך Internet Explorer 5 על מערכות ההפעלה Windows 2000, Windows NT 4.0, Windows 98, או Windows 95.

שיעור 3:
הגדרה והפעלה של שירותי Telnet

ב-Windows 2000, Telnet מספק למשתמשים תמיכה בפרוטוקול Telnet, חלק ממערכת TCP/IP. Telnet הוא פרוטוקול לגישה מרחוק, בו ניתן להשתמש לכניסה למחשב מרוחק, התקן רשת, או רשת TCP/IP פרטית. Telnet Server ו- Telnet Client פועלים יחד ומאפשרים למשתמשים לתקשר עם מחשב מרוחק. ב- Windows 2000, Telnet Server מותקן כשירות, ושמו Telnet. שירות Telnet מאפשר למשתמשים בלקוח Telnet להיכנס למחשב המפעיל את שירות Telnet, ולהפעיל יישומים טקסטואליים (Character-Mode) על מחשב זה. שירות Telnet פועל כשער, דרכו יכולים מחשבים המפעילים לקוח Telnet לתקשר זה עם זה. לקוח Telnet מאפשר למשתמשים להתחבר למחשב מרוחק ולתקשר עם מחשב זה דרך חלון מסוף.

לאחר שיעור זה, תוכל

- להגדיר את שירות Telnet 2000 של Windows 2000, כדי לאפשר גישה ממחשב המפעיל לקוח Telnet.
- להשתמש ב- Telnet Client להתחברות לשירות Telnet.

זמן לימוד משוער: 25 דקות

שירות Telnet

שירות Telnet של Windows 2000 מאפשר למשתמשים בלקוח Telnet להתחבר למחשב המפעיל את שירות Telnet, ולהשתמש בפקודות משורת הפקודה על המחשב, כאילו היו יושבים מולו. לקוחות Telnet יכולים להתחבר לשרת, להיכנס לשרת זה, ולהפעיל יישומים טקסטואליים (Character-Mode). שירות Telnet גם פועל כשער עבור לקוחות Telnet להתקשרות זה עם זה. מחשב המפעיל שירות Telnet יכול לתמוך ב-עד 63 מחשבי לקוח Telnet בזמן נתון כלשהו.

רשיון חיבור שרת Telnet

לכל התקנה של Windows 2000 Server מצורפים שני רשיונות חיבור לשירות Telnet. הדבר מגביל את שירות Telnet לחיבור שני לקוחות Telnet בו-זמנית. אם דרושים רשיונות נוספים, ניתן להשתמש בשירות Telnet מחבילת התוספת Windows Services for UNIX.

אימות Telnet

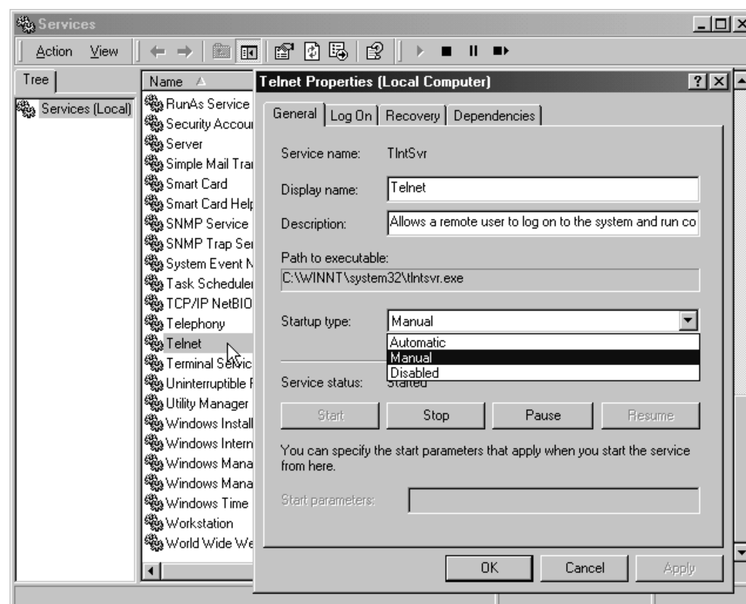
ניתן להשתמש בשם המשתמש ובסיסמה המקומיים של Windows 2000, או במידע של domain account לצורך גישה אל שרת Telnet. שיטת האבטחה משולבת באבטחת Windows 2000. אם לא משתמשים באפשרות האימות NTLM (**NT L**AN **M**anager), שם המשתמש והסיסמה נשלחים לשרת Telnet כטקסט רגיל.

אם משתמשים באימות NTLM, הלקוח משתמש בהקשר האבטחה של Windows 2000 לאימות, והמשתמש אינו מתבקש להזין שם וסיסמה. שם המשתמש והסיסמה מוצפנים.

הערה אם מוגדרת האפשרות User Must Change Password At Next Logon עבור משתמש, המשתמש אינו יכול להיכנס לשירות Telnet כאשר מופעל אימות NTLM. על המשתמש להיכנס ישירות לשרת ולשנות את הסיסמה, ורק אז יוכל להיכנס באמצעות לקוח Telnet.

הפעלה והפסקה של שרת Telnet

בהתקנה בתצורת ברירת מחדל של Windows 2000 Server, שירות Telnet מוגדר להפעלה ידנית. ניתן להשתמש בתוסף התוכנה Services או בתוסף התוכנה Computer Management להפעלה, הפסקה, או הגדרה של שירות Telnet להפעלה אוטומטית. תרשים 14.18 מציג את תיבת הדו-שיח Telnet Properties עבור שירות Telnet.



תרשים 14.18 דף Telnet Properties מציג את אפשרויות Startup Type עבור שירות שרת זה.

בתוסף התוכנה Computer Management, Telnet הוא שירות הממוקם תחת הצומת Services and Applications. בחר Services מחלון Tree, ואז בחר Telnet מרשימת השירותים בחלון הפרטים.

ניתן גם להפעיל או להפסיק את שירות Telnet משורת הפקודה. כדי להתחיל את Telnet Server, הקלד **net start tlntsvr** או **net start telnet** בשורת הפקודה, ואז הקש Enter. להפסקת Telnet Server, הקלד **net stop tlntsvr** או **net stop telnet** בשורת הפקודה, ואז הקש Enter.

תוכנית השירות Admin של שרת Telnet

ניתן להשתמש בתוכנית השירות Telnet Server Admin להפעלה, הפסקה, או קבלה של מידע אודות Telnet Server. ניתן גם להשתמש בה לקבלת רשימת משתמשים עדכניים, הפסקת שימוש של משתמש, או שינוי הגדרות רישום המערכת (Registry) של Telnet Server.

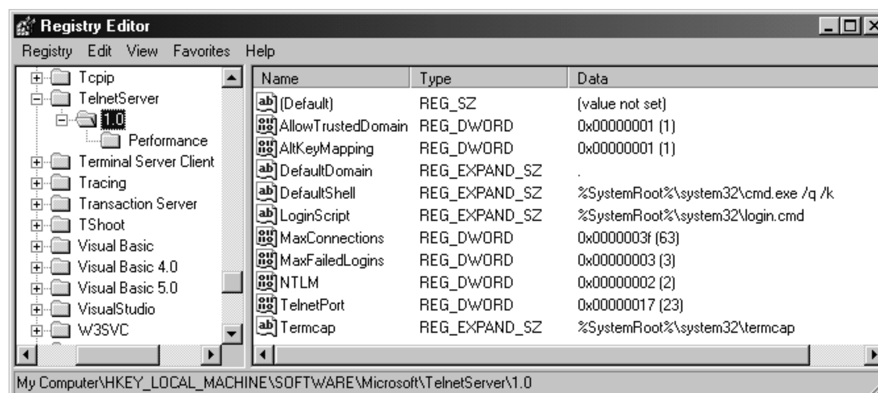
אזהרה עריכה שגויה של רישום המערכת עלולה לגרום נזק חמור למערכת. לפני ביצוע שינויים ברישום המערכת, מומלץ מאוד לגבות נתונים חשובים כלשהם המצויים במחשב.

לפתיחת תוכנית השירות Telnet Server Admin, לחץ על כלי Telnet Administration בקבוצת התוכניות Administrative Tools או לחץ Start, לחץ Run, הקלד **tlntadmn**, ואז לחץ OK. אם לא ניתן לפתוח את תוכנית השירות Telnet Server Admin, ייתכן שיהיה צורך להתקין את חבילת Administration Tools (Adminpak.msi).

הטבלה הבאה מציגה את אפשרויות תוכנית השירות Telnet Server Administration.

אפשרות	שם	תיאור
0	Quit this application	מסיים את ה-session של תוכנית השירות Telnet Server Admin.
1	List the current users	מציג רשימה של המשתמשים הנוכחיים, כולל שם המשתמש, domain, כתובת מחשב מרוחק, זיהוי session וזמן יומן.
2	Terminate a user session	מסיים את ה-session של משתמש מסוים שנבחר.
3	Display/change registry settings	מספק רשימה של הגדרות רישום, אותן ניתן לשנות. ראה בטבלה הבאה.
4	Start the service	מתחיל את שירות Telnet server.
5	Stop the service	מפסיק את שירות Telnet Server.

שינויים ברישום המערכת המבוצעים באמצעות תוכנית השירות Telnet Server Admin משנים הגדרות המאוחסנות במפתח רישום המערכת הבא במחשב שרת Telnet: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\TelnetServer\1.0. מיקום זה ברישום המערכת מוצג בתרשים 14.19.



תרשים 14.19 הגדרות Telnet Server אותן ניתן לשנות באמצעות תוכנית השירות Telnet Server Admin.

הטבלה הבאה מציגה את הגדרות Telnet Server שאותן ניתן לשנות:

אפשרות	שם	תיאור	ערך ברירת מחדל
0	Exit this menu	יוצא מהתפריט וחוזר לאפשרויות המקוריות של תוכנית השירות Telnet Server Administration.	N/A
1	AllowTrusted Domain	משנה את ערכו הנוכחי של Trusted Domain.	1
2	AltKeyMapping	משנה את הערך הנוכחי.	1
3	DefaultDomain	מגדיר את ברירת המחדל של Domain name.	. (נקודה פירושה ה-domain הנוכחי של שרת Telnet).

אפשרות	שם	תיאור	ערך ברירת מחדל
4	DefaultShell	מציג את מיקום הנתיב עבור התקנת הסביבה.	%systemroot%\System32 \Cmd.exe /q /k מתג q/ מאפשר הד (echo) ומתג k/ מבצע פקודה, אך אינו סוגר את חלון שורת הפקודה.
5	LogonScript	מציג את מיקום הנתיב והשם עבור קובץ תסריט כניסת לקוח גלובלי לשירות Telnet. כברירת מחדל קובץ זה ממפה את לקוח Telnet לספריית הבית, אם מוגדרת כזו בפרופיל המשתמש.	%systemroot%\System32 \login.cmd
6	MaxFailedLogins	מציג את המספר המירבי של ניסיונות כניסה כושלים לפני סיום החיבור.	3
7	NTLM	מציג את המספר הנוכחי של כניסות מותרות באימות NTLM.	2
8	TelnetPort	מציג את ברירת המחדל של Telnet Server.	23

הערה הגדרת הרישום Termcap מציינת את המיקום של קובץ TermCap (**Term**inal **Cap**abilities), המשמש מספר תוכניות שירות של מסוף לקוח, לקבוע כיצד להזיז את הסמן בזמן Terminal session.

כאשר משנים את ה-Default domain account, ההגדרה משפיעה רק לאחר התחלה מחדש של שירות Telnet. יש להיכנס כחבר בקבוצה Administrators לשימוש בתוכנית השירות Telnet Server Administration.

פתרון בעיות

הטבלה הבאה מציגה מידע אודות מספר בעיות נפוצות, העלולות להתרחש בעת הפעלת Telnet Server.

הודעת שגיאה	גורם	פתרון
Invalid input	הערך שהוזן איננו חוקי	בדוק את טווח הערכים האפשריים, והזן מחדש את הערך הרצוי.
Failed to open the registry key	שרת Telnet חייב לפעול לפתיחת מפתח הרישום. שגיאה זו מצביעה על כך שהוא איננו פועל כעת.	הפעל את שירות Telnet.
Failed to query the registry value	שרת Telnet חייב לפעול לשאילתה של ערך רישום. שגיאה זו מצביעה על כך שהוא אינו פועל כעת.	הפעל את שירות Telnet.

לקוח Telnet

ניתן להשתמש ב- Microsoft Telnet Client להתחברות למחשב מרוחק המפעיל שירות Telnet או לתוכנת שרת Telnet אחרת. לאחר ההתחברות, ניתן לתקשר עם שרת Telnet. סוג ה-session שיתבצע תלוי באופן הגדרת תוכנת Telnet. תקשורת, משחקים, ניהול מערכת, והדמיות כניסה מקומית הם רק חלק מהשימושים האופייניים ב-Telnet.

לקוח Telnet משתמש בפרוטוקול Telnet המהווה חלק ממערכת הפרוטוקולים TCP/IP, להתחברות למחשב מרוחק על פני רשת. תוכנת לקוח Telnet מאפשרת למחשב להתחבר לשרת מרוחק. ניתן להשתמש בלקוח Telnet, המסופק עם Windows 2000 להתחברות אל מחשב מרוחק, לכניסה אל מחשב מרוחק ולאינטראקציה עם מחשב מרוחק, כאילו אתה יושב מולו.

משתמשים בגרסאות קודמות של לקוח Telnet של Microsoft יבחינו במספר שינויים בגירסה המצורפת ל- Windows 2000. השינוי הבולט ביותר הוא שלקוח Telnet של Microsoft הוא עתה יישום שורת פקודה, במקום יישום חלונאי. כיישום שורת פקודה,

לקוח Telnet של Microsoft ייראה מוכר מאוד למשתמשים בלקוחות Telnet מבוססי UNIX.

תכונה חשובה חדשה בלקוח Telnet של Microsoft היא תמיכה באימות NTLM. בעזרת תכונה זו, מחשב המשתמש בלקוח Telnet של Microsoft יכול להתחבר למחשב Windows 2000 המפעיל את שירות Telnet באמצעות אימות NTLM.

הערה לקוח Telnet של Microsoft אינו תומך ברישום יומן של telnet session.

שימוש ב- Telnet

לפתיחת Telnet, לחץ Start, לחץ Run, והקלד **telnet**. ניתן גם להקליד **telnet** בשורת הפקודה. לשימוש ב-Telnet, חייב להיות מותקן ומוגדר פרוטוקול TCP/IP על המחשב, וחייב להיות לך חשבון משתמש על מארח מרוחק.

להצגת עזרה עבור Telnet, הקלד **help**, בשורת הפקודה של Microsoft Telnet. להתחברות לאתר, הקלד **connect <computer_name>** כאשר <computer_name> הוא כתובת IP או שם המארח של המחשב המפעיל את שירות Telnet.

תרגיל 2: הגדרה והתחברות לשירות Telnet

בתרגיל זה תגדיר את שירות Telnet שיתחיל על Server01. אז, תתחבר לשירות Telnet מ- Server01 ותוודא את החיבור. בצע שיעור זה מ-Server01.

הערה אם אתה מפעיל Server02, תוכל לבצע את הליך 2 מ-Server02.

הליך 1: אפשור והגדרה של שירות Telnet

בהליך זה תגדיר את שירות Telnet להפעלה אוטומטית, ואז תפעיל את שירות Telnet.

1. היכנס ל-Server01 בשם משתמש Administrator עם הסיסמה password.
2. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על Services.

   יופיע מסוף Services.
3. בחלונית הפרטים, גלול מטה ולחץ לחיצה כפולה על Telnet. תופיע תיבת הדו-שיח Telnet Properties (Local Computer).
4. בתיבת הרשימה הנפתחת Startup Type שנה את הערך מ-Manual ל-Automatic.
5. תחת Service status, לחץ על לחצן Start. תופיע תיבת Service Control status לזמן קצר, תוך התחלת שירות Telnet.
6. לחץ OK לסגירת תיבת הדו-שיח Telnet Properties (Local Computer).
7. סגור את Services Console.

הליך 2: שימוש בלקוח Telnet של Microsoft

בהליך זה תתחבר לשירות Telnet מלקוח Telnet של Microsoft. ניתן לבצע הליך זה על Server01 או על Server02. ביצוע ההליך מ-Server02 מספק גישה מרחוק אל Server01. אולם, למטרות תרגול, הפעלת פקודות אלו מ-Server01 מספיקה. אם אתה מבצע את ההליך מ-Server02, עליך להיכנס בשם משתמש Administrator לפני שתתחיל.

1. לחץ Start, ולחץ Run. תופיע תיבת הדו-שיח Run.
2. בתיבת הטקסט Open, הקלד **telnet** ולחץ OK. תופיע שורת הפקודה Microsoft Telnet.
3. הקלד **help** או **?** להצגת רשימת הפקודות הזמינות. תופיע רשימה של הפקודות הנתמכות.
4. הקלד **open server01**. תופיע הודעת ברכה Welcome to Microsoft Telnet Server.

הערה ניתן להשתמש בקיצורים עבור הפקודות שמזינים. לדוגמה, **O server01** שווה ל- **open server01**.

5. פקודות כלשהן שניתן להפעיל משורת הפקודה של Server01, ניתן כעת להפעיל מסביבת Telnet.
6. השאר את Telnet פעיל בעת ביצוע ההליך הבא.

הליך 3: הפעלת כלי הניהול של שרת Telnet

בהליך זה תנטר את שירות Telnet למציאת חיבורי לקוח Telnet, ואז תנתק את לקוח Telnet המחובר באמצעות Telnet Server Administrator.

1. לחץ Start, ולחץ Run. תופיע תיבת הדו-שיח Run.
2. בתיבת הטקסט Open, הקלד **tlntadmn** ולחץ OK. יופיע חלון פקודות תוכנית השירות Telnet Server Admin.
3. הקלד **1** להצגת רשימה של המשתמשים הנוכחיים. תופיע סטטיסטיקה עבור המשתמש Administrator.
4. הקלד **2** להפסקת השירות עבור משתמש. תופיע הודעה המורה להזין session ID של משתמש להפסקת session זה.
5. הקלד **1**, זה ה-session ID עבור המשתמש המחובר. תופיע שוב רשימת אפשרויות עבור הפקודה.
6. חזור אל חלון לקוח Telnet על Server01 או Server02. שים לב שהחיבור עם המארח ניתק.

7. לחץ על מקש כלשהו כדי להמשיך. חזרת לחלון הפקודה של לקוח Telnet של Microsoft.
8. הקלד **q** או **quit** לסגירת חלון הפקודה של Microsoft Telnet Client.
9. חזור אל חלון הפקודה של Telnet Server Administrator.
10. הקלד **0** לסגירת Telnet Server Administrator.

סיכום שיעור

שירות Telnet ולקוח Telnet פועלים יחד, כדי לאפשר למשתמשים לתקשר עם מחשב מרוחק. שירות Telnet של Windows 2000 מאפשר למשתמשים בלקוח Telnet של Microsoft להתחבר מרחוק למחשב, ולהשתמש ביישומים משורת הפקודה על המחשב, כאילו הם יושבים מולו. ניתן להשתמש בתוסף התוכנה Services, בתוסף התוכנה Computer Management, או בשורת הפקודה, להפעלה או להפסקה של שירות Telnet. בנוסף, ניתן להשתמש בתוכנית השירות Telnet Server Admin להפעלה, הפסקה, או קבלה של מידע אודות שירות Telnet. ניתן גם להשתמש בו לקבלת רשימה של משתמשים פעילים, להפסקת session של משתמש, או לשינוי הגדרות רישום של שירות Telnet. לקוח Telnet של Microsoft מאפשר להתחבר למחשב מרוחק המפעיל תוכנת שרת Telnet. קיימת תמיכה באימות NTLM, כאשר לקוח Telnet של Microsoft מתחבר לשירות Microsoft Telnet. Telnet מספק תמיכת משתמש עבור פרוטוקול Telnet, פרוטוקול גישה מרחוק שבו ניתן להשתמש להתחברות למחשב מרוחק, התקן רשת, או רשת פרטית.

שיעור 4:
התקנה והגדרה של שירותי Telnet

שירותי המסוף (Terminal Services) מספקים גישה ל-Windows 2000 וליישומים מבוססי Windows העדכניים ביותר עבור מחשבי לקוח. הם גם מספקים גישה לשולחן העבודה ויישומים המותקנים בכל מקום, מכל לקוח נתמך. שירותי המסוף הם תכונה מובנית של Windows 2000, המאפשרת למנהלי טכנולוגיית המידע ולמנהלי מערכות להגביר את הגמישות בהפעלת יישומים, לשלוט על עלויות ניהול מחשב ולנהל מרחוק משאבי רשת.

לאחר שיעור זה, תוכל

- להפעיל את שירותי המסוף בסביבת Windows 2000.

זמן לימוד משוער: 40 דקות

סקירה כללית של שירותי המסוף

שירותי המסוף (Terminal Services) הפועלים על Windows 2000 Server מאפשרים הפעלת יישומי לקוח, עיבוד נתונים, ואחסון נתונים על השרת. הם מספקים גישה מרחוק לשולחן העבודה של שרת באמצעות תוכנת הדמיית מסוף (Terminal Emulation Software). את תוכנת הדמיית המסוף ניתן להפעיל על מספר התקני חומרת לקוח, כגון מחשב אישי, מחשב כף-יד מבוסס Windows CE, או מסוף.

בעזרת שירותי המסוף, תוכנת ההדמייה של המסוף שולחת הקשות מקשים ותנועות עכבר אל השרת. שירותי המסוף מבצעים את כל הטיפול בנתונים באופן מקומי על השרת, ומעבירים חזרה את התצוגה. גישה זו מאפשרת בקרה מרחוק על שרתים וניהול יישומים מרכזי, תוך הפחתת דרישות רוחב הפס של הרשת בין השרת ללקוח.

משתמשים יכולים לגשת אל שירותי המסוף על פני כל חיבור TCP/IP, כולל גישה מרחוק, Ethernet, אינטרנט, אלחוט, רשת מרחבית - WAN (**W**ide **A**rea **N**etwork), או רשת וירטואלית פרטית - VPN (**V**irtual **P**rivate **N**etwork). פעילות המשתמש מוגבלת רק על ידי הקישור האיטי ביותר בחיבור, ואבטחת החיבור נשלטת על ידי יישום TCP/IP במרכז הנתונים.

שירותי המסוף מספקים ניהול מרחוק של משאבי רשת, פעילות אחידה למשתמשים בסניפי הארגון במיקומים מרוחקים, או ממשק גרפי ליישומים עסקיים על מחשבים מבוססי טקסט.

שירותי המסוף הם תכונה מובנית של Windows 2000. ניתן להפעיל את שירותי המסוף באחד משני מצבים: ניהול מרחוק (Remote Administration) או שרת יישומים (Application Server).

ניהול אדמיניסטרטיבי מרחוק

ניהול מרחוק (Remote Administration) מספק למנהלי מערכת שיטה חזקה לניהול מרחוק של כל מחשב Windows 2000 Server על פני כל חיבור TCP/IP. ניתן לנהל שיתוף קבצים ומדפסות, לערוך את הרישום (Registry) ממחשב אחר ברשת, או לבצע משימה כלשהי, כאילו אתה יושב פיסית מול השרת. ניתן להשתמש במצב ניהול מרחוק לניהול שרתים שאינם תואמים בדרך כלל עם מצב שרת יישומים של שירותי המסוף, כמו למשל שרתים המפעילים את השירות Cluster.

מצב ניהול מרחוק מתקין רק את רכיבי הגישה מרחוק של שירותי המסוף. הוא אינו מרכיב רכיבי שיתוף יישומים. פירוש הדבר שניתן להשתמש בניהול מרחוק עם תקורה מעטה מאוד על שרתים קריטיים למשימה. שירותי המסוף מאפשרים עד שני חיבורים בו-זמניים לניהול מרחוק. לא נדרש רישוי נוסף כלשהו עבור חיבורים אלה, ואין צורך בשרת רשיונות (License Server).

הערה למידע נוסף אודות ניהול מרחוק, ראה בתקליטור המצורף לספר זה (\chapt14\articles\TSRemote.doc).

שרת יישומים

במצב שרת יישומים (Application Server), ניתן להפעיל ולנהל יישומים ממיקום מרכזי, תוך חיסכון בזמן פיתוח והפעלה של מנהלים, בנוסף לחיסכון בזמן ובמאמץ הדרושים לתחזוקה ולשדרוג. לאחר שיישום הופעל בשירותי המסוף, לקוחות רבים יכולים להתחבר - באמצעות חיבור גישה מרחוק, LAN או WAN, ומסוגי לקוחות רבים ושונים.

ניתן להתקין יישומים ישירות בשרת מסוף (Terminal Server), או להשתמש בהתקנה מרחוק. לדוגמה, ניתן להשתמש בשירותי Group Policy ו- Active Directory לפרסום חבילות יישומי Windows Installer אל שרת מסוף או אל קבוצה של שרתי מסוף. ניתן להתקין יישומים על ידי Administrator בלבד, על בסיס שרת (Per Server Basis), ורק אם מופעלת הגדרת Group Policy המתאימה.

נדרש רישוי לקוחות בעת הפעלת שרת מסוף כשרת יישומים. כל מחשב לקוח, ללא קשר לפרוטוקול המשמש להתחברות לשרת המסוף, חייב להיות בעל רשיון Terminal Services Client Access License בנוסף לרשיון Windows 2000 Client Access.

הערה למידע אודות אופטימיזציה של יישומים עבור Windows 2000 Terminal Services, ראה בתקליטור המצורף לספר זה (\chapt14\articles\TSAppDev.doc).

כלים לניהול

כדי לסייע בהתקנת שירותי המסוף עבור Windows 2000, נוספו כלי ניהול נוספים לתיקיה Administrative Tools, כולל Terminal Services Client Creator, Terminal Services Manager, Terminal Services Configuration, ו- Terminal Services Licensing.

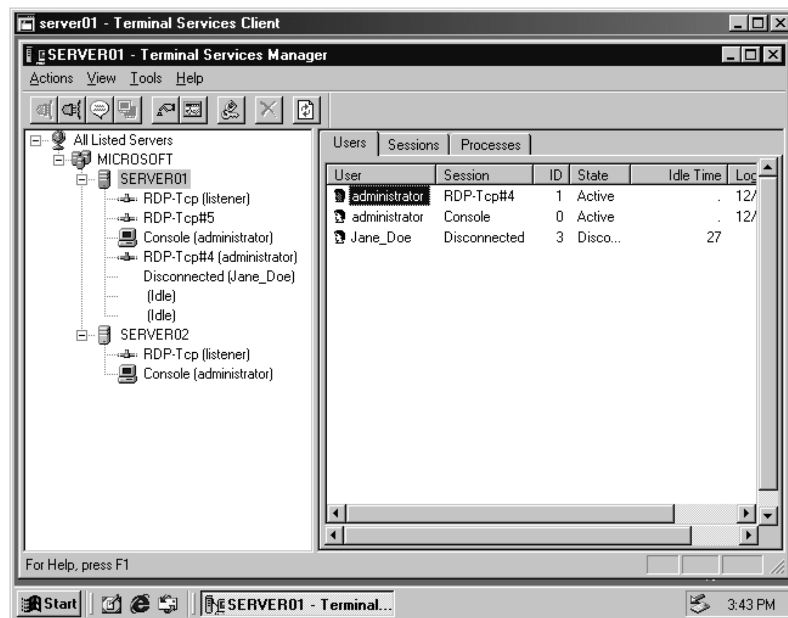
הערה Terminal Services Licensing מותקן רק אם נבחר מצב Application Server או אם מותקן Adminpak.msi.

Terminal Services Client Creator

השתמש בכלי זה ליצירת דיסקטים להתקנת תוכנת לקוח שירותי מסוף (Terminal Services Client) על פלטפורמות Windows for Workgroups, Windows 95, Windows 98 ו- Windows NT.

Terminal Services Manager

בעזרת כלי זה, ניתן לנהל את כל שרתי Windows 2000 המפעילים שירותי מסוף. מנהלים יכולים להציג משתמשים פעילים, שרתים, והליכים . בנוסף, מנהלים יכולים לשלוח הודעות למשתמשים מסוימים, להשתמש בתכונת Remote Control, ולסיים תהליכים. תרשים 14.20 מציג את מסוף Terminal Services Manager הפועל בתוך Terminal Services session.



תרשים 14.20 הפעלת Terminal Services Manager לניהול שירותי מסוף הפועלים על Server01.

Terminal Services Configuration

כלי זה מאפשר לנהל את הגדרות **R**emote **D**esktop **P**rotocol (RDP). שינוי אפשרויות בכלי זה יהיה גלובלי, אלא אם בוחרים לרשת מידע מאותן אפשרויות הממוקמות בהגדרות המשתמש. האפשרויות הזמינות כוללות הגדרת הצפנת חיבור, הגדרות כניסה, פסקי זמן (Time-Outs), תוכניות ראשוניות המופעלות עם כניסה מוצלחת, אפשרויות שליטה מרחוק, מיפוי מדפסת Windows, מיפוי יציאות LPT, מיפוי לוח, ויישום אפשרויות אלו על מתאם LAN מסוים.

Terminal Services Licensing

בעזרת כלי זה, מאחסנים ועוקבים אחר רשיונות גישת לקוח Windows 2000 Terminal Services. ניתן להתקין כלי זה בעת התקנת שירותי מסוף או מאוחר יותר. כאשר לקוחות מתחברים לשירותי מסוף, שירותי המסוף מאמתים את רשיון הלקוח. אם ללקוח אין רשיון, או שהוא מבקש רשיון חלופי, שירותי מסוף מבקשים רשיון משרת הרשיונות. שרת הרשיונות מספק רשיון מהמאגר של רשיונות זמינים, ושירותי המסוף מעביר את הרשיון ללקוח. אם אין רשיונות זמינים, שרת הרשיונות מעניק רשיון זמני עבור הלקוח. לאחר הענקתו, כל רשיון לקוח מקושר עם מחשב או מסוף מסוימים.

הערה למידע נוסף אודות כלי ניהול Terminal Services, ראה בתקליטור המצורף לספר זה (\chapt14\articles\TSsol.doc).

רכיבי רישוי לשירותי המסוף

לשירותי המסוף יש שיטה עצמאית לרישוי לקוחות המתחברים לשרתי המסוף. שיטה זו נפרדת משיטת הרישוי המשמשת לקוחות Windows 2000 Server. רישוי שירותי מסוף כולל ארבעה רכיבים: Microsoft Clearinghouse, שרת רשיונות, שרת מסוף ורשיונות לקוחות.

Microsoft Clearinghouse

Microsoft Clearinghouse הוא מסד הנתונים ש- Microsoft מתחזקת להפעלת שרתי רשיונות ולהנפקת חבילות מפתח רשיון לקוח עבור שרתי הרשיונות המבקשים אותן. המסלקה (Clearinghouse) מאחסנת מידע אודות כל שרתי הרשיונות הפעילים וחבילות מפתח רשיון הלקוח שהונפקו. ניתן לגשת אל המסלקה באמצעות האשף Licensing בתוסף התוכנה Terminal Services Licensing.

שרת רשיונות

שרת רשיונות (License Server) מאחסן את כל רשיונות לקוח שירותי מסוף שהותקנו עבור שרת מסוף, ועוקב אחר הרשיונות שהונפקו למחשבי לקוח או מסופים. שרת מסוף חייב להיות מסוגל להתקשר לשרת רשיונות פעיל, לפני שניתן להנפיק רשיונות ללקוחות. שרת רשיונות פעיל יחיד יכול לשרת מספר שרתי מסוף.

שרת מסוף

שרת מסוף (Terminal Server) הוא המחשב שעליו מאופשרים ופועלים שירותי מסוף. הוא מספק גישת לקוחות ליישומים מבוססי Windows הפועלים לחלוטין על השרת, ותומך במספר Client Sessions על השרת. כאשר לקוחות נכנסים לשרת מסוף, השרת מאמת את רשיון הלקוח. אם ללקוח אין רשיון, שרת מסוף מבקש רשיון עבור לקוח זה משרת הרשיונות.

רשיונות לקוחות

לכל מחשב לקוח או מסוף המתחברים לשרת מסוף חייב להיות רשיון לקוח תקף. רשיון הלקוח (Client License) מאוחסן באופן מקומי ומוצג לשרת מסוף, בכל פעם שהלקוח מתחבר לשרת. השרת מאמת את הרשיון, ואז מאפשר ללקוח להתחבר.

הערה למידע נוסף אודות רישוי Terminal Services, ראה בתקליטור המצורף לספר זה (\chapt14\articles\TSLicensing.doc).

ניהול שרת הרשיונות

הפעלת שרת הרשיונות של שירותי מסוף כוללת הגדרת שרת הרשיונות, אפשור השרת, הפעלת השרת והתקנת הרשיונות.

הגדרת שרת רשיונות

שרת רשיונות דרוש לשירותי המסוף בעת הפעלה במצב שרת יישומים. שירות הרישוי של שירותי המסוף הוא שירות בעל השפעה קטנה, המאחסן את רשיונות הלקוח שהונפקו עבור שרת מסוף, ועוקב אחר הרשיונות שהונפקו למחשבי לקוח או מסופים.

את שרת הרשיונות יש להפעיל באמצעות Microsoft Clearinghouse, ויש לטעון אותו ברשיונות גישת לקוח (Client Access Licenses) להפצה מהמסלקה (Clearinghouse). הגישה אל שרת הרשיונות מתבצעת על ידי שרתי מסוף רק לצורך הנפקת רשיון חדש, ויש צורך לנהל שרת רשיונות לצורך קבלת רשיונות מהמסלקה.

אפשור שרת רשיונות

ניתן לאפשר את שירות Terminal Services Licensing על המחשב, כאשר מפעילים את Windows 2000 Server Setup. בסביבת ייצור מומלץ לאפשר את שירותי המסוף על שרת חבר או על שרת עצמאי, ולהתקין את שרת הרשיונות על מחשב אחר. שירותי המסוף דורשים משאבים רבים.

קיימים שני סוגים של שרתי רשיונות: שרת רשיונות Domain ושרת רשיונות ארגון. לפני התקנת שרת הרשיונות, כדאי לשקול איזה משני סוגי שרתי הרשיונות דרוש:

- ❖ **Domain license server** – מתאים אם רוצים לתחזק שרת רשיונות נפרד עבור כל Domain. אם יש קבוצות עבודה או תחומי Windows NT 4.0, שרת רשיונות Domain הוא הסוג היחיד שניתן להתקין. שרתי מסוף יכולים לגשת לשרתי רשיונות Domain, רק אם הם נמצאים באותו domain כמו שרת הרשיונות. כברירת מחדל, שרת רשיונות מותקן כשרת רשיונות Domain.
- ❖ **Enterprise license server** – יכול לשמש שרתי מסוף ב-Domain כלשהו בתוך אתר, אולם ה-Domain חייב להיות Windows 2000 Domain. השרת יכול לשמש רק שרתי מסוף באותו אתר. סוג שרת רשיונות זה מתאים אם יש תחומים רבים. ניתן להתקין שרתי רשיון ארגון רק באמצעות Add/Remove Programs. לא ניתן להתקין אותם במהלך תוכנית ההתקנה של Windows 2000.

כאשר מחליטים היכן ברשת הפיסית להפעיל את שרת הרשיונות, יש לשקול כיצד שרת מסוף מגלה ומתקשר עם שרת רשיונות. עם הפעלת שירותי המסוף מתחיל שרת המסוף לדגום (Polling) את ה-Domain ואת שירותי Active Directory, בחיפוש אחר שרת רשיונות (בסביבת קבוצות עבודה, שרת מסוף משדר לכל השרתים בקבוצת העבודה על אותה Subnet).

הערה בתחומי Windows 2000, שרת רשיונות domain **חייב להיות מותקן** על DC. **בקבוצות** עבודה **או** בתחומי Windows NT 4.0, **ניתן להתקין** את שרת **רשיונות** Domain על שרת כלשהו. אם מתכננים לעבור בעתיד מקבוצת עבודה **או** Windows NT 4.0 Domain ל-Windows 2000 Domain, כדאי לשקול להתקין את שרת הרשיונות על מחשב שניתן לשדרוג ל-Windows 2000 Domain Server.

להפעלת שרת הרשיונות במהירות ולגישה אל Microsoft Clearinghouse דרך האינטרנט, התקן את השרת על מחשב בעל גישת אינטרנט.

יש לאפשר את שרת הרשיונות של Windows 2000 בתוך 90 יום מאפשור שירותי המסוף של Windows 2000. אם לא אפשרת את שירות הרישוי לפני תום תקופה זו, יחדלו שירותי המסוף של Windows 2000 מלפעול.

הפעלת שרת רשיונות

יש להפעיל שרת רשיונות לצורך זיהוי השרת, וכדי לאפשר לו להנפיק רשיונות לקוח לשרתי Terminal. ניתן להפעיל שרת רשיונות באמצעות אשף Licensing.

קיימות ארבע דרכים להפעלת שרת הרשיונות :

- אינטרנט
- על בסיס Web
- פקס
- טלפון

אם המחשב המפעיל את תוסף התוכנה Terminal Services Licensing מחובר לאינטרנט, שיטת ההפעלה באמצעות האינטרנט היא המהירה והפשוטה ביותר. אשף Licensing מכוון אותך אל אתר אינטרנט המאובטח של Microsoft, שבו מופעלים שרתי רשיונות. כאשר מפעילים שרת רשיונות, Microsoft מספקת לשרת תעודה דיגיטלית המאמתת את בעלות וזהות השרת. באמצעות תעודה זו, שרת רשיונות יכול לבצע פעולות נוספות עם Microsoft ולקבל רשיונות גישת לקוח עבור שרתי Terminal.

אם לשרת הרשיונות אין קישוריות אינטרנט, אולם קיימת יכולת לגשת ל- World Wide Web באמצעות דפדפן על מחשב אחר, ניתן להפעיל את שרת הרשיונות על בסיס Web. אשף Licensing מכוון אותך לאתר Web המאובטח של Microsoft לקבלת תעודה עבור שרת הרשיונות.

שיטות חלופיות להפעלת שרת רשיונות כוללות שליחת המידע בפקס או התקשרות למרכז תמיכת לקוחות הקרוב. אשף Licensing מנחה אותך גם בשלבים אלה. ניתן לאתר את מספר הטלפון או הפקס המתאימים להתקשרות באמצעות אשף Licensing. אם משתמשים בשיטת הפעלה באמצעות פקס, הבקשה המאושרת מוחזרת בפקס מ-Microsoft. אם משתמשים בהפעלה באמצעות הטלפון, הבקשה נענית על ידי נציג שירות לקוחות בטלפון.

יש צורך להפעיל שרת רשיונות פעם אחת בלבד. בעת המתנה להשלמת תהליך ההפעלה, שרת הרשיונות יכול להנפיק רשיונות זמניים ללקוחות המאפשרים להם להשתמש בשרתי Terminal למשך עד 90 יום.

התעודה הדיגיטלית המזהה באופן ייחודי את שרת הרשיונות שלך מאוחסנת בצורת **מזהה שרת רשיונות** (License Server ID). שמור עותק של מספר זה במיקום בטוח. להצגת המספר לאחר שהופעל שרת הרשיונות, האר את שרת הרשיונות, ובחר Properties מהתפריט View. הגדר את שיטת התקשורת ל- World Wide Web, ולחץ OK. אז בחר Install Licenses מהתפריט Action, ולחץ Next. License Server ID רשום במרכז מסך Licensing Wizard.

התקנת רשיונות

רשיונות של שירותי המסוף חייבים להיות מותקנים על שרת הרשיונות, כדי שהגדרת Internet Connector תהיה זמינה, או כדי שלקוחות שאינם Windows 2000 יוכלו לגשת באופן קבוע לשרת Windows 2000 Terminal. כדי לקבל רשיונות גישת לקוח לשירותי המסוף של Windows 2000 או רשיונות Internet Connector, יש לרכוש אותם בדרך המקובלת לרכישת תוכנה. לאחר הרכישה ניתן להתקין את הרשיונות באמצעות אשף Licensing.

לאחר התקנת הרשיונות, שרת הרשיונות יכול להתחיל להפעיל אותם. לקוחות עם רשיונות זמניים של 90 יום ישודרגו לרשיון גישת לקוח שירותי המסוף, בפעם הבאה שהם נכנסים למערכת (אלא אם מספר רשיונות גישת הלקוח המותקנים קטן ממספר הרשיונות הזמניים שהונפקו).

הפצה למחשבי לקוח

מחשבי לקוח או מסופים מתחברים לשרת Terminal באמצעות תוכנית לקוח קטנה המותקנת בדיסק או ב-Firmware. הברירה באיזו פלטפורמת לקוח להשתמש, תלויה בבסיס המותקן הנוכחי ובצרכי הלקוח המסוים. כדרישה בסיסית יש לוודא שכל מחשב לקוח או מסוף, הצפויים להתחבר לשרת Terminal, מסוגלים פיסית לארח את תוכנת הלקוח ולהתחבר על פני הרשת.

מחשבי לקוח מבוססי Windows המתחברים לשירותי המסוף זקוקים למעבד 80386 לפחות, במהירות 33MHz (למרות שמומלץ 486/66), כרטיס וידיאו VGA 16 סיביות, ומחסנית Microsoft TCP/IP. לקוח שירותי מסוף פועל על Windows 2000, Windows for Workgroups 3.11, Windows 95, Windows 98 ו- Windows NT 3.51 או מאוחר יותר.

לקוח שירותי המסוף צורך רק כ- 500KB מקום בדיסק, ובדרך כלל משתמש בכ- 4MB זיכרון RAM בעת הפעלה. אם מאופשר מטמון סיביות לקוח, ייתכן שיהיה שימוש בעוד כ- 10MB מקום בדיסק. לביצועים הטובים ביותר, מחשב המפעיל לקוח שירותי מסוף זקוק לסף 8MB זיכרון RAM פיסי, או יותר תחת Windows for Workgroups 3.11 או Windows 95, 24MB או יותר, עבור Windows 98, ו- 32MB או יותר, עבור Windows 2000.

הערה לקוח שירותי המסוף עבור התקני Windows CE **ניתן למצוא בתקליטור ההתקנה של** Windows 2000 Server **בתיקיה** \Valueadd\msft\mgmt\mstsc_hpc\.

תוכנת לקוח RDP מותקנת כברירת מחדל כרכיב משנה של שירותי המסוף. הלקוחות השונים מותקנים בספריה %systemroot%\system32\clients\tsclient.

קיימות שתי דרכים להפעלת לקוח:

- ❖ יצירת שיתוף קובץ לביצוע התקנה דרך הרשת.
- ❖ בחירת Terminal Services Client Creator מהתפריט Administrative Tools, ויצירת דמות לקוח שאותה ניתן להתקין באמצעות דיסקט.

הערה לקוח שירותי המסוף זקוק ל- TCP/IP כדי להתחבר לשרת, אולם שירותי המסוף עצמם יכולים להשתמש ב- IPX לקבלת גישה לשרתי Novell, במידת הצורך.

הגדרות לקוח

ניתן לבצע מיטוב של שירותי המסוף, תוך התייחסות להמלצות הבאות:

- ❖ בטל את Active Desktop.
- ❖ בטל גלילה חלקה (Smooth Scrolling).
- ❖ הפחת את השימוש בגרפיקה ואנימציה, כולל גרפיקה מונפשת, שומרי מסך, סמנים מהבהבים, ו- Microsoft Office Assistant המונפש. הצב קיצורי דרך על שולחן העבודה, ושמור את תפריט Programs שטוח ככל שניתן. הימנע משימוש במפות סיביות בטפט; ב- Display Properties, הגדר את Wallpaper ל- None בכרטיסיה Background, ובחר צבע יחיד עבור הכרטיסיה Appearance.
- ❖ אפשר שיתוף קבצים על מחשבי לקוח ושתף כוננים עם שמות קלים לזיהוי כגון "drivec". שים לב להשלכות האבטחה הנובעות מכך.
- ❖ הימנע משימוש ביישומי MS-DOS או Win 16 (16 סיביות) היכן שניתן.
- ❖ הגדר את שרת Terminal, כך שיחזיר את שם הכניסה של המשתמש במקום את שם המחשב ליישומים המשתמשים בפונקציית NetBIOS המבקשת את שם המחשב.
- ❖ הכשר משתמשים לשימוש בצירופי מקשים חמים של שירותי המסוף. קיימים מספר הבדלים חשובים בין מקשים חמים המשמשים ב-Terminal Services client session, למקשים חמים ב-Windows 2000 Session.

שדרוג ל- שירותי המסוף

הגישה בה תנקוט ביחס לשדרוג לשירותי המסוף תלויה בהגדרות שירותי המסוף הקיימות.

WinFrame עם או ללא MetaFrame

אין כל נתיב שדרוג ישיר מ- WinFrame לשירותי מסוף. במקרה זה יש לשדרג תחילה ל- Microsoft Terminal Server 4.0 ואז לשדרג ל- Windows 2000.

Terminal Server 4.0 ללא MetaFrame

כאשר Terminal Server 4.0 מותקן, קיים נתיב שדרוג ישיר לשירותי המסוף. כאשר מתקינים את Windows 2000, השרת מזהה את מהדורת Terminal Server 4.0, מבצע שדרוג אוטומטי, ומאפשר אוטומטית את שירותי המסוף במצב Application Server. שים לב שייתכן שתצטרך להתקין מחדש יישומים קיימים, אם תאפשר את שירותי המסוף במצב Application Server.

Terminal Server 4.0 עם MetaFrame

שדרוג מ- Terminal Server 4.0 עם MetaFrame דומה לשדרוג מ- Terminal Server 4.0, אלא שלאחר השדרוג ל-Terminal Server יש לשדרג את MetaFrame לגירסה המעודכנת ביותר של MetaFrame Windows 2000.

Windows NT ללא שירותי מסוף

כאשר מתקינים את Windows 2000, יש לבחור את שירותי המסוף במצב Remote Administration או Application, כדי לאפשר את פעולת השירותים.

התקנה והגדרה של יישומים

שרת Windows 2000 שהוגדר להפעלת שירותי מסוף במצב Application Server מספק מספר חיבורי משתמשים בו-זמניים למספר יישומים כלשהו.

מומלץ להוסיף או להסיר יישומים באמצעות היישומון Add/Remove Programs תחת לוח הבקרה. הליך זה מנהל אוטומטית את דרישות ההתקנה של שירותי המסוף. ניתן גם להתקין יישומים ישירות על ידי העברת השרת למצב Install.

להעברת שרת מסוף למצב Install, הקלד **change user /install**. לאחר השלמת התקנת התוכנה, הקלד **change user /execute** להחזרת שרת המסוף למצב הפעלה.

פקודות Change User אינן נחוצות כאשר משתמשים ב- Add/Remove Programs, מכיון ש- Add/Remove Programs מטפל בהליך זה ברקע. עדיף להשתמש ביישומון Add/Remove Programs כיון שתמיד קיימת האפשרות לשגיאה או השמטה בעת שימוש בשורות פקודה. אם יישום מותקן ללא שימוש ב- Add/Remove Programs, ובלי להשתמש בשורת הפקודה להגדרת מצב Install, יש להסיר את היישום ולהתקינו מחדש.

רק למנהלים מותר להתקין יישומים על שרת יישומים של שירותי המסוף.

הפעלת יישומים באמצעות Group Policy

הפעלת יישומים באמצעות שירותי Active Directory ו- Group Policy, על ידי שימוש ב- Windows Installer היא שיטת הפעלת יישומים גמישה מאוד. היא מאפשרת התקנה וניהול יישומים במספר דרכים שונות. שלוש דרכים עיקריות שבהן ניתן להפעיל יישומים בעת שימוש ב- Windows Installer הן:

- התקנה על המחשב המקומי על ידי המשתמש.
- הקצאה על ידי מנהל המערכת מ-DC למשתמש או מחשב.
- פרסום על ידי מנהל המערכת מ-DC עבור משתמש.

לפני שניתן להתקין יישום באמצעות Windows Installer, חייבת להיות חבילת התקנה MSI. זמינה עבור היישום.

הפעלת יישומים מ-DC

להפעלת יישום מ-DC, צריך מנהל המערכת להקצות יישום מבוסס MSI. למחשב. שרתי יישומים אינם יכולים להקצות או לפרסם יישומים למשתמשים.

דרושים קבצי המרה אם חבילת התקנת היישום המקורית לא התקינה את כל רכיבי היישום הדרושים על הדיסק המקומי. קבצי המרה מאפשרים לבחור מה, אם בכלל, צריך להתקין בעת ההתקנה.

מנהל מערכת יכול גם להתקין יישום מ-Remote Session או MMC Console של שרת היישומים. יוזמה להתקנה אופיינית מתחילה בשימוש בפקודה הבאה:

Msiexec/I *ApplicationName*.MSI
TRANSFORMS=*TransformFileName*.MST ALLUSERS=1

התקנת יישום בסביבה מרובת משתמשים שונה מאוד מהתקנה עבור משתמש יחיד. אסור שהתקנת תוכנת שרת יישומים תסכן את המערכת הפעילה, ויש להגדיר את ההתקנה, כך שתאפשר משתמשים בו-זמניים. לכן, רק מנהלים יכולים להתקין יישומים, ומשתמשים אינם יכולים להתקין דבר.

באחריות כל מנהל מערכת להחליט איזה יישומים דרושים, ולהבטיח שיישומים מותקנים מקומית וזמינים, לפני אפשור חיבורי משתמשים מרוחקים.

תרגיל 3: התקנה והגדרה של שירותי המסוף ורשיונות

בתרגיל זה תתקין את שירותי המסוף של Windows 2000, ואז תפעיל ניהול מרוחק מ-Server02 ל-Server01. אז, תתקין את Terminal Services Licensing ותקים Terminal Session מ-Server02 ל-Server01.

הליך 1: התקנת שירותי המסוף והפעלת Remote Administration

בהליך זה תתקין את שירותי המסוף להפעלה במצב Remote Administration על Server01. אז תפעיל remote administration session מ-Server02. ודא שתקליטור התקנת Windows 2000 נמצא בכונן התקליטורים על Server01.

1. היכנס ל-Server01 בשם משתמש Administrator עם הסיסמה password.
2. לחץ Start, הצבע על Settings ולחץ על Control Panel.
3. בלוח הבקרה, לחץ לחיצה כפולה על היישומון Add/Remove Programs. תופיע תיבת הדו-שיח Add/Remove Programs.
4. בחלונית השמאלית, לחץ על Add/Remove Windows Components. לאחר זמן קצר, יוצג אשף Windows Components.
5. גלול מטה, סמן את תיבת הסימון Terminal Services ולחץ Next. יופיע מסך Terminal Services Setup.
6. קרא את המידע במסך זה, ודא שלחצן האפשרות Remote Administration Mode מסומן ולחץ Next.

   יופיע מסך Configuring Components בעת ש-Windows 2000 מגדירה ומתקינה רכיבים. לאחר מספר דקות, יופיע מסך אשף Completing the Windows Components Wizard.
7. לחץ Finish. תופיע תיבת הדו-שיח Add/Remove Programs.

8. לחץ Close וסגור את לוח הבקרה. תופיע תיבת הודעה System Setting Change, ובה הודעה שעליך להפעיל מחדש את המחשב, לפני שההגדרות ייכנסו לתוקף.

9. לחץ Yes להפעלת המחשב מחדש.

10. לאחר ש-Server01 מתחיל מחדש, אל תיכנס למערכת. היכנס למערכת מ-Server02 תוך שימוש בניהול מרחוק של שירותי המסוף.

11. מ- Server02, היכנס ל-Server01 בשם משתמש Administrator עם הסיסמה password. ודא שאתה נכנס ל-Domain בשם MICROSOFT.

12. לחץ Start, ולחץ Run. תופיע תיבת הדו-שיח Run.

13. בתיבת הטקסט Open, הקלד **\\server01\c$\Program Files\terminal services client**, ולחץ OK.

    יופיע חלון Terminal Services Client.

14. לחץ לחיצה כפולה על הסמל Conman. יופיע Client Connection Manager.

15. לחץ על הסמל הראשון בסרגל הכלים. אשף Client Connection Manager יתחיל.

16. לחץ Next. יופיע מסך Create A Connection.

17. בתיבת הטקסט Connection Name, הקלד **Server01 Remote Administration**.

18. בתיבת הטקסט Server name or IP Address הקלד **Server01** ולחץ Next.

    יופיע מסך Automatic Logon.

19. סמן את תיבת הסימון Logon Automatically With This Information.

20. בתיבת הטקסט User Name, הקלד **administrator**.

21. בתיבת הטקסט Password, הקלד **password**.

22. בתיבת הטקסט Domain, הקלד **microsoft** ולחץ Next. יופיע מסך Screen Options.

23. בחר רזולוציה בה מסוגל הצג של Server02 לתמוך. אם אינך יודע את הרזולוציה של הצג, סמן את לחצן האפשרות 640x480.

24. לחץ Next. יופיע מסך Connection Properties.

25. סמן את תיבות הסימון Enable Data Compression ו- Cache Bitmaps, ולחץ Next.

    יופיע המסך Starting A Program.

26. לחץ Next. יופיע מסך Icon And Program Group.

27. לחץ Next. יופיע מסך Completing The Client Connection Manager Wizard.

28. לחץ Finish. יופיע Client Connection Manager עם החיבור החדש שיצרת.

29. לחץ לחיצה כפולה על סמל Server01 Remote Administration.

תופיע תיבה Connecting. ייפתח חלון מסוף שהכותרת שלו היא SERVER01 - Terminal Services Client (Server01 Remote Administration).

30. בתיבת הדו-שיח Log On To Windows, הקלד **password** ואז לחץ OK.

כעת תוכל לנהל מרחוק את Server01 מ-Server02. שים לב שעל צג Server01, המחשב אינו מחובר, אולם אתה מחובר ל-Server01 מ-Server02.

31. סגור את חלון SERVER01 - Terminal Services Client Console (Server01 Remote Administration), המופיע על Server02.

תופיע תיבת הודעה Disconnecting Windows Session, ובה הודעה שכעת תתנתק מ-Server01, אולם תוכל לחזור ל-Session זה מאוחר יותר, ולהמשיך להפעיל תוכניות שהותחלו ב-terminal session זה.

32. לחץ OK.

33. סגור את Client Connection Manager, וסגור את חלון לקוח שירותי המסוף.

הליך 2: התקנת Terminal Services Licensing

בהליך זה תתקין Terminal Services Licensing (שירותי רישוי מסופים) על Server01, כדי לשרת את דרישות הרשיונות של מצב Application Server. ודא שתקליטור התקנת Windows 2000 Server נמצא בכונן התקליטורים על Server01.

הערה בסביבת ייצור, מומלץ להתקין שירותי רשיונות על מחשב שאינו מפעיל גם את שירותי המסוף במצב Application Server.

---

1. היכנס ל- Server01 בשם משתמש Administrator עם הסיסמה password.
2. לחץ Start, הצבע על Settings, ולחץ על Control Panel.
3. בלוח הבקרה, לחץ לחיצה כפולה על היישומון Add/Remove Programs. תופיע תיבת הדו-שיח Add/Remove Programs.
4. בחלונית השמאלית, לחץ על Add/Remove Windows Components. לאחר זמן קצר, יופיע אשף Windows Components.
5. גלול מטה, סמן את תיבת הסימון Terminal Services Licensing ולחץ Next. יופיע מסך Terminal Services Setup.
6. סמן את לחצן האפשרות Application Server Mode, ולחץ Next.

   יופיע מסך Terminal Services Setup ובו הודעה שייתכן ש- Windows 2000 Administration Tools לא יפעל כנדרש לאחר התקנת שירותי המסוף במצב Application Server.

7. לחץ Next. יופיע מסך Terminal Services Licensing Setup.
8. לחץ על לחצן האפשרות Your Entire Enterprise.

   שים לב שמסד הנתונים של שרת הרשיונות יאוחסן בתיקיה C:\WINNT\System32\LServer.

9. לחץ Next. יופיע מסך Configuring Components בעת ש-Windows 2000 מגדירה ומתקינה רכיבים. לאחר מספר דקות, יופיע מסך אשף Completing the Windows Components Wizard.
10. לחץ Finish. תופיע תיבת הדו-שיח Add/Remove Programs.

11. לחץ Close, ואז סגור את לוח הבקרה.

תופיע תיבת הודעה System Setting Change, ובה הודעה שעליך להפעיל מחדש את המחשב לפני שההגדרות ייכנסו לתוקף.

12. לחץ Yes להפעלת המחשב מחדש.

13. היכנס ל-Server01 בשם משתמש Administrator עם הסיסמה password.

14. לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על Terminal Services Licensing.

יופיע תוסף התוכנה Terminal Services Licensing ותיבת המצב Terminal Services Licensing Manager תופיע בעת איתור שירותי המסוף. לאחר מציאת Server01, הוא יופיע בחלונית הפרטים במצב Not Activated.

15. בחלונית הפרטים, לחץ על SERVER01.

16. פתח את תפריט Action, ואז לחץ על Activate Server. יופיע אשף Licensing.

17. לחץ Next. יופיע מסך Connection Method.

18. בתיבת הרשימה הנפתחת Connection Method, בחר Telephone, ולחץ Next.

יופיע מסך Country/Region Selection.

19. בחר מדינה, ולחץ Next.

20. בלי להכניס קוד זיהוי שרת רשיונות, לחץ Next.

תופיע תיבת הודעה של Licensing Wizard ובה הסבר שקוד זיהוי שרת הרשיונות שהוזן אינו תקף, או שלא הוזן.

21. לחץ OK.

22. במסך License Server Activation, לחץ Cancel.

23. סגור את תוסף התוכנה Terminal Services Licensing.

רכיב Terminal Services Licensing מותקן, ותוכל להשתמש בשירותי המסוף במצב Application Server למשך 90 יום. לפני תום 90 הימים, עליך להפעיל את השרת בעזרת תוסף התוכנה Terminal Services Licensing והמידע שסופק לך על ידי חברת Microsoft.

הליך 3: הכנת יישום לפעולה במצב Terminal Services Application

בהליך זה, תסיר את ההתקנה של Windows 2000 Administration Tools ואז תתקין אותם מחדש, כדי להבטיח שהם פועלים נכון מ-Terminal session. ודא שתקליטור התקנת Windows 2000 Server נמצא בכונן התקליטורים על Server01, ושנכנסת ל-Server01 בשם משתמש Administrator.

1. ב-Server01, לחץ Start, הצבע על Settings ולחץ על Control Panel.
2. בלוח הבקרה, לחץ לחיצה כפולה על היישומון Add/Remove Programs. תופיע תיבת הדו-שיח Add/Remove Programs.
3. בתיבה Currently Installed Programs, לחץ על Windows 2000 Administration Tools, ולחץ על הלחצן Remove.

   תופיע תיבת ההודעה Add/Remove Programs, ובה שאלה האם ברצונך להסיר את Windows 2000 Administration Tools מהמחשב שלך.

4. לחץ Yes. תופיע תיבת מצב Windows Installer, ואז תיבת המצב Windows 2000 Administration Tools בעת הסרת הכלים.

   תיבת הדו-שיח Add/Remove Programs אינה מכילה עוד את Windows 2000 Administration Tools.

5. בחלונית השמאלית, לחץ על Add New Programs.
6. מהחלון העיקרי, לחץ על CD or Floppy.

   יופיע מסך Install Program From Floppy Disk or CD-ROM.

7. לחץ Next. יופיע מסך Run Installation Program.
8. בתיבת הטקסט Open, הקלד **<cd-rom>:\i386\adminpack.msi** כאשר <cd-rom> היא אות הכונן עבור כונן התקליטורים.
9. לחץ Next.

   תופיע תיבת המצב Windows Installer, ואז תופיע תיבת המצב Windows 2000 Administration Tools Installation. לאחר מספר רגעים, יופיע אשף Windows 2000 Administration Tools Setup.

10. לחץ Next. יופיע מסך Installation Progress בעת ההתקנה.

    לאחר מספר רגעים, יופיע אשף Completing the Windows 2000 Administration Tools Setup.

11. לחץ Finish. יופיע מסך After Installation.
12. לחץ Next. יופיע מסך Finish Admin Install.

13. קרא את הטקסט במסך זה, ולחץ Finish. תופיע תיבת הדו-שיח Add/Remove Programs.

14. לחץ על לחצן Close.

15. סגור את לוח הבקרה.

הליך 4: התחברות לשירותי המסוף במצב שרת יישומים והקצאת כלי שירותי מסוף

בהליך זה תתקין את לקוח שירותי מסוף על Server02, ואז תפעיל מסך מסוף מ-Server02 אל Server01. בתוך ה-terminal session הפועל על Server02, תנטר את ה-session באמצעות כלים המותקנים על Server01. יש להיכנס תחילה ל-Server01 ול-Server02 בשם משתמש Administrator ב-domain בשם MICROSOFT.

1. על Server01 לחץ Start, ולחץ Run. תופיע תיבת הדו-שיח Run.

2. בתיבת הטקסט Open, הקלד **C:\winnt\system32\clients** ולחץ OK. יופיע החלון Clients.

3. לחץ על התיקיה Tsclient.

4. פתח את תפריט File, ולחץ Sharing. תופיע תיבת הדו-שיח Tsclient Properties עם הכרטיסיה Sharing פעילה.

5. לחץ על לחצן האפשרות Share This Folder. יופיע Tsclient בתיבת הטקסט Share Name.

6. לחץ OK.

7. סגור את החלון Clients.

8. על Server02 לחץ Start, ולחץ Run. תופיע תיבת הדו-שיח Run.

9. בתיבת הטקסט Open, הקלד **\\server01\tsclient** ולחץ OK. יופיע החלון Tsclient On Server01.

10. לחץ לחיצה כפולה על התיקיה win32.

11. לחץ לחיצה כפולה על התיקיה disks.

12. לחץ לחיצה כפולה על התיקיה disk1.

13. לחץ לחיצה כפולה על הסמל setup. יופיע מסך Terminal Services Client Setup.

14. לחץ על Continue. תופיע תיבת הדו-שיח Name And Organization Information.

15. הקלד את שמך, ולחץ OK. תופיע תיבת ההודעה Confirm Name And Organization Information.

16. לחץ OK. תופיע תיבת הודעה License Agreement.

17. לחץ על הלחצן I Agree. תופיע תיבת הדו-שיח Terminal Services Client Setup.

שים לב שתוכנת הלקוח תותקן תחת התיקיה Program Files.

18. לחץ על הלחצן הגדול להתקנת תוכנת Terminal Services Client.

תופיע תיבת ההודעה Terminal Services Client Setup ובה שאלה, האם רצונך שהליך התקנה זה יחול על כל המשתמשים במחשב זה.

19. לחץ Yes. ההתקנה מתקדמת ואז תופיע תיבת ההודעה Terminal Services Client Setup, ובה הודעה שההתקנה הסתיימה בהצלחה.

20. לחץ OK.

21. סגור את החלון Disk1.

22. ב-Server02, לחץ Start, הצבע על Programs, הצבע על Terminal Services Client, ולחץ על הסמל Terminal Services Client.

תופיע תיבת הדו-שיח Terminal Services Client.

23. בתיבת הרשימה הנפתחת Server, הקלד **Server01**.

24. השאר את אזור המסך 640x480, ודא שתיבת הסימון Enable Disk Compression נבחרה, וסמן את תיבת הסימון Cache Bitmaps To Disk.

25. לחץ על הלחצן Connect. יופיע החלון Server01 - Terminal Services Client.

26. בתיבת הדו-שיח Log On To Windows, הקלד **Jane_Doe** עם סיסמה של **student**, ואז לחץ OK.

שים לב שמוצג הפרופיל האישי של Jane_Doe, דבר המיוצג על ידי הצבעים המותאמים אישית.

27. מתוך ה-Terminal session, לחץ Start, הצבע על Programs, הצבע על Administrative Tools, ולחץ על Terminal Services Manager.

בתוסף התוכנה SERVER01 - Terminal Services Manager מתחיל בתוך ה-Terminal session.

28. בחלון Tree, לחץ על SERVER01.

29. בחלונית הפרטים, לחץ על Jane_Doe.

30. פתח את תפריט Actions, ולחץ Status. יופיע מידע מצב אודות ה-session של Jane_Doe.

31. לחץ על הלחצן Close.

32. פתח את תפריט Actions, ולחץ על Send Message. תופיע תיבת הדו-שיח Send Message.

33. בתיבת הכותרת העליונה Message, הקלד **Message from the Administrator** ובתיבת Message התחתונה, הקלד -

Terminal Services will be shutting down for maintenance in a few minutes. Please Close your session

34. לחץ OK. תופיע תיבת הודעה מה-administrator ב-terminal session.

35. לחץ OK.

36. סגור את תוסף התוכנה SERVER01 - Terminal Services Manager ואז סגור את חלון SERVER01 - Terminal Services Client.

    תופיע תיבת ההודעה Disconnect Windows Session.

37. קרא את ההודעה ולחץ OK.

38. סגור את Server01 ואת Server02.

סיכום שיעור

Terminal Services הפועל על שרת Windows 20000 מאפשר ביצוע כל יישומי לקוח, עיבוד נתונים ואחסון נתונים על השרת. הוא מספק גישה מרחוק לשולחן עבודה של שרת באמצעות תוכנת הדמיית מסוף. ניתן לאפשר את שירותי המסוף (Terminal Services) באחד משני מצבים: ניהול מרחוק (Remote Administration) ושרת יישומים (Application Server). ניהול מרחוק מספק למנהלי מערכות שיטה חזקה לניהול מרחוק של כל שרת Windows 2000 על פני כל חיבור TCP/IP. במצב שרת יישומים, ניתן להפעיל ולנהל יישומים ממקום מרכזי, תוך חיסכון בזמן פיתוח והפעלה של המנהלים בנוסף לחיסכון בזמן ובמאמץ הדרושים לתחזוקה ושדרוגים. שירות הרשיונות של שירותי המסוף כולל ארבעה רכיבים: Microsoft Clearinghouse, שרת רשיונות, שרת מסוף (Terminal Server) ורשיונות לקוחות. הפעלת שרת רשיונות של שירותי המסוף כוללת הגדרת שרת הרשיונות, אפשורו, הפעלתו והתקנת הרשיונות. לכל מחשב לקוח או מסוף הצפויים להתחבר לשרת מסוף חייבת להיות יכולת פיסית לארח את תוכנת הלקוח ולהתחבר על פני רשת. שרת Windows 2000 המוגדר להפעלת שירותי המסוף במצב שרת יישומים (Application Server) מספק מספר חיבורי משתמשים בו-זמנית למספר יישומים כלשהו. ניתן להפעיל יישומים באמצעות שירותי Active Directory ו- Group Policy, וניתן להפעיל יישומים מ-DC. כאשר מתקינים את שירותי המסוף עבור Windows 2000, נוספים לתיקיה Administrative Tools כלי ניהול, כולל Terminal Services Client Creator, Terminal Services Manager, Terminal Services Configuration, ו- Terminal Services Licensing.

שאלות סיכום

השאלות הבאות מיועדות לחיזוק הנושאים העקרים שנידונו בפרק זה. אם אינך יודע את התשובה לשאלה, חזור ועיין בשיעורים המתאימים, ונסה לענות על השאלה שנית. תשובות לשאלות נמצאות בנספח A. לנוחיותך השאלות מופיעות באנגלית ואח״כ בעברית.

1. Compare a virtual directory to a Dfs root.
2. You are accessing the IIS 5.0 documentation from Internet Services Manager (HTML) . All of the documentation appears and you are able to access information via the Index tab. Under the Index tab, you find the phrase Process Accounting. However, when you perform a search on this phrase, the Web browser reports that your search phrase cannot be found. What is the most likely reason that this is happening?
3. You have created a virtual directory for the purpose of WebDAV publishing. The home directory of the Web site is accessible from Internet Explorer 5 but when you attempt to access the virtual directory for WebDAV publishing, access is denied. Name two reasons why this may happen and how you can solve this access problem.
4. Why is it important that the Microsoft Telnet Client and the Microsoft Telnet service support NTLM authentication?
5. If Terminal Services is not licensed, what features of Terminal Services will work and for how long?

1. השווה בין ספריה וירטואלית לבין Dfs root.
2. אתה ניגש לתיעוד IIS 5.0 מתוך Internet Services Manager (HTML). כל התיעוד נראה ואתה יכול לגשת למידע באמצעות הכרטיסיה Index. תחת הכרטיסיה Index, אתה מוצא את הביטוי Process Accounting. אולם, כאשר אתה מבצע חיפוש לפי ביטוי זה, הדפדפן מדווח שביטוי חיפוש זה לא נמצא. מה הסיבה הסבירה ביותר לכך?
3. יצרת ספריה וירטואלית למטרות פרסום WebDAV. תיקיית הבית של אתר האינטרנט נגישה מ- Internet Explorer 5, אולם כאשר אתה מנסה לגשת לספריה הוירטואלית לפרסום WebDAV, הגישה נדחית. ציין שתי סיבות להתרחשות אפשרית של מצב זה, וכיצד ניתן לפתור בעיית גישה זו.
4. מדוע חשוב ש- Microsoft Telnet Client ושירות Microsoft Telnet יתמכו באימות NTLM?
5. אם שירותי המסוף פועלים ללא רשיון, איזה תכונות של שירותי המסוף יפעלו, ולמשך כמה זמן?

נספחים

חלק זה כולל:

- שלושה נספחים באנגלית
- מילון מונחים (Glossary) באנגלית
- אינדקס באנגלית.

שים לב, הנספח הראשון מתחיל בעמוד 2 שנמצא בסוף הספר (לפני הקטלוג המצורף) ומתקדם משמאל לימין לתוך הספר.

Appendixes

Appendix A

Questions and Answers

Chapter 1

Review

1. A client has asked you to recommend the appropriate server edition(s) of Windows 2000 for his environment. Your recommendation is based on the following characteristics:

    - All remote offices are connected to the corporate headquarters and data center by high-speed (greater than 10 Mbps) connections.
    - All 10,000 users run Windows 2000 Professional or Windows 98.

    And the following functional requirements:

    - All sites will access a high-availability server cluster running a Microsoft SQL Server 7.0 database. A two-server cluster with six processors per computer is adequate, and there are no plans to upgrade the cluster.
    - All other servers will run an edition of Windows 2000 to provide Active Directory services, basic file and print services, and dial-in access to the network.
    - These servers will run anywhere between one to four processors. Processor sizing will be based on the number of users supported at each site. For example, a small remote site will contain a single processor server while all servers in the corporate site will contain four processors. For simplicity, one server edition of Windows 2000 will be selected for all computers serving this role.
    - Each domain in Active Directory services will support 2,500 users.

Windows 2000 Advanced Server is recommended for the SQL Server two-node cluster. Windows 2000 Advanced Server supports two-node clustering, eight-way SMP, and high availability. Windows 2000 Datacenter is also an option; however, this edition of the operating system exceeds the customer's requirements for clustering and SMP. Windows 2000 Server will not meet the customer's requirements for the SQL Server application because it does not support clustering or six-way SMP.

All other servers should run Windows 2000 Server because it meets the customer's requirements for a maximum of 4-way SMP, Active Directory services, dial-in via RAS, and file and print services. It easily scales to support 2,500 users/domain and over 10,000 users in the network.

2. Why is a WDM driver preferred over legacy Windows NT drivers?

   WDM device drivers benefit from a common set of WDM I/O services. Therefore, a driver developed using the WDM driver development model should be binary-compatible with Windows 2000 and Windows 98.

   The WDM driver model is based on a class/miniport structure that provides modular, extensible architectures for device support. This model allows each WDM class to abstract many of the common details involved in controlling similar devices.

3. How does Windows 2000 protect Executive services from user mode applications?

   User mode applications request system services through the appro-priate subsystem. The subsystem then makes a request on behalf of the application to the Windows 2000 Executive running in Kernel mode. While system services are available to both user mode sub-systems and other components of the Windows 2000 Executive, the subsystem or component must call the exported support routine to make a request for Executive service.

4. What component of the Executive makes Windows 2000 preemptible?

   The Process Manager suspends and resumes threads of running processes. This is an important feature of any multitasking operating system because the Process Manager will not allow a properly functioning process to monopolize the operating system and therefore stop all other processes from running.

5. What is the primary difference between a workgroup and a domain?

   A workgroup is a distributed directory maintained on each computer within the workgroup. A domain is a centralized directory of re-sources maintained on domain controllers and presented to the user through Active Directory services.

6. What is the structure and purpose of a directory service?

   A directory service consists of a database that stores information about network resources, such as computer and printers, and the services that make this information available to users and applications.

Chapter 2

Review

1. If you are installing Microsoft Windows NT in a dual-boot configuration on the same computer, which file system should you choose? Why?

   The best choice is FAT. Although both Windows 2000 and Windows NT support NTFS, Windows 2000 supports advanced features pro-vided by NTFS 5.0. For example, file encryption is supported in NTFS 5.0, but previous versions of NTFS did not support file encryption. Therefore, when Windows NT is running on a dual-boot computer, it will not be able to read encrypted files created in Windows 2000.

2. Which licensing mode should you select if users in your organization require frequent access to multiple servers? Why?

   Per Seat licensing is the best choice for this environment. A Per-Seat license is more expensive per client computer than Per-Server licensing but becomes much less expensive when many client computers access several servers. If Per-Server licensing is used in this environment, each server must be individually licensed for client computer access.

3. You are installing Windows 2000 Server on a computer that will be a member server in an existing Windows 2000 domain. You want to add the computer to the domain during installation. What information do you need, and what computers must be available on the network, before you run the Setup program?

You need the DNS domain name of the domain that you are joining. You must also make sure that a computer account for the member server exists in the domain or you must have the user name and password of a user account in the domain with the authority to create computer accounts in the domain. A server running the DNS. service and a domain controller in the domain you are joining must be available on the network. If dynamic IP addressing is configured during setup, a server supporting DHCP must be available to assign an address to the computer.

4. You are using a CD-ROM to install Windows 2000 Server on a computer that was previously running another operating system. There is not enough space on the hard disk to run both operating systems, so you have decided to repartition the hard disk and install a clean copy of Windows 2000 Server. Name two methods for repartitioning the hard disk.

   Answer 1: Use a disk partitioning tool like MS-DOS fdisk to remove any existing partitions, and then create and format a new partition for the Windows 2000 installation.

   Answer 2: Start the computer by booting from the Windows 2000 Server Setup disk. During the text-mode portion of installation, you can delete the partition and then create and format a new one. Con-tinue the installation of Windows 2000 Server to the new partition.

5. You are installing Windows 2000 over the network. Before you install to a client computer, what must you do?

   Locate the path to the shared installation files on the distribution server. Create a 671-MB FAT partition on the target computer (2 GB recommended). Create a client disk with a network client so that you can connect from the computer, without an operating system, to the distribution server.

6. A client is running Windows NT 3.5 Server and is interested in upgrad-ing to Windows 2000. From the list of choices, choose all possible upgrade paths:

   a. Upgrade to Windows NT 3.51 Workstation and then to Windows 2000 Server.

   b. Upgrade to Windows NT 4.0 Server and then to Windows 2000 Server.

   c. Upgrade directly to Windows 2000 Server.

d. Run Convert.exe to modify any NTFS partitions for file system compatibility with Windows 2000, and then upgrade to Windows 2000 Server.

e. Upgrade to Windows NT 3.51 Server and then to Windows 2000 Server.

Answer: b and e

Answer a is wrong because Windows NT Workstation (3.*5x* or 4.0) cannot be upgraded to Windows 2000 Server.

Answer c is wrong because Windows NT 3.5 cannot be directly upgraded to Windows 2000 Server.

Answer d is wrong because the Windows 2000 Setup process auto-matically upgrades NTFS to NTFS version 5.0.

7. In your current network environment, user disk space utilization has been a major issue. Describe three services in Windows 2000 Server to help you manage this issue.

   Answer 1: Disk quotas in NTFS version 5.0 allow you to control per-user disk space usage by disk.

   Answer 2: Disk compression allows you to compress data at the disk, directory, or file level. Disk compression does not affect a user's allocated quota. Quotas are calculated based on the uncompressed file size.

   Answer 3: Remote Storage Services provides an extension to disk space by making removable media accessible for file storage. Infre-quently used data is automatically archived to removable media. Archived data is still easily accessible to the user; however, data retrieval is slower than with unarchived data.

Chapter 3

5. What folder appears directly under the win2000dist folder that does not appear in the i386 folder? (Page 115)

   oem

16. What is the purpose of the UDF file? (Page 116)

    The UDF file allows each automated setup to be customized with the unique settings contained in the file. To start an unattended setup, the UniqueID contained in the UDF file is specified on the command line. During setup the unique data in the UDF file is merged into the answer file.

Review

1. What is the purpose of using the /tempdrive: or /t: installation switches with Winnt32.exe or Winnt.exe, respectively?

   The Winnt32.exe /tempdrive: switch and the Winnt.exe /t: switch copy the Windows 2000 Server installation files to the drive specified with the switch. For example, Winn32.exe /tempdrive:d copies all Windows 2000 installation files to the D: partition. Using this switch also tells Setup which partition should be the boot partition for the installation of Windows 2000 Server.

2. You are asked to develop a strategy for rapidly installing Windows 2000 Server for one of your clients. You have assessed their environment and have determined that the following three categories of computers require Windows 2000 Server:

   ❖ There are 30 unidentical computer configurations currently running Windows NT Server 4.0 that need to be upgraded to Windows 2000 Server.

   ❖ There are 20 identical computers that need a new installation of Windows 2000 Server.

   ❖ Remote sites will run a clean installation of Windows 2000 Server. You want to make sure that they install a standard image of Win-dows 2000 Server that is consistent with your local configuration of the operating system. You will provide them with hard disks that they will install in their servers.

   What are the steps for your installation strategy?

For the 30 computers that need to be upgraded, build an answer file and a distribution share using Setup Manager. Further customize the answer file with a text editor. Use a product such as SMS to auto-mate the distribution of operating system upgrades. If SMS is not available, run winnt32 with the /unattend switch and the other switches described in Lesson 1 that are designed to automate the installation process.

For the 20 identical computers, set up one computer with the operating system and all applications that you need to replicate on all other computers. Copy sysprep.exe, sysprepcl.exe, and sysprep.inf (answer file format) into the $OEM\$1\Sysprep folder. Make sure the [GuiRunOnce] section of the answer file calls sysprep.exe with the -quiet switch to continue the setup without any user interaction. Create an image with a third-party image utility, and copy this image to each of the 20 identical computers. Upon reboot, Mini-Setup will run using information in sysprep.inf to complete the setup.

For the remote sites, use /Syspart to prepare the disks for the second half of the installation. Ship the disks to the remote sites and instruct the local administrators to install them in their servers as the bootable drive, usually by setting the SCSI ID to 0 or 7, depending on the SCSI hardware.

You can also use the bootable CD-ROM method. If you use this method, include a floppy disk containing the winnt.sif file to auto-mate Setup.

3. What is the purpose of the OEM folder and the subfolders created beneath it by Setup Manager?

   The oem folder contains the optional cmdlines.txt file and subfolders for original equipment manufacturer (OEM) files and other files needed to complete or customize automated installation. Folders below oem hold all files that are not part of a standard installation of Windows 2000 Server. These folders map to specific partitions and directories on the computer running an unattended installation. The following list describes the purpose of each folder below oem:

   $$ – copies files from this distribution folder location to $windir$ or $systemroot$. For a standard installation of Windows 2000 Server, these variables map to C:\Winnt. There are other folders below this one too, such as Help for OEM help files and System32 for files that must be copied to the System32 directory.

$1 – copies files from this distribution folder location to the root of the system drive. This location is equivalent to the %systemdrive% variable. In a typical installation of Windows 2000 Server, this variable maps to the C:\ root. The $1 folder contains a drivers folder for third-party driver installation.

Drive letter – folders named after a specific drive letter map to the drive letter on the local computer. For example, if you need to copy files to the E: drive during setup, create an E folder and place files or folders in this folder.

Textmode – contains any special HALs or mass storage device drivers required for installing and running Windows 2000 Server.

4. How does Cmdlines.txt differ from [GuiRunOnce]?

   Cmdlines.txt runs commands before a user is logged on and in the context of the system account. Any command line or installation that can occur without a user logon can complete using Cmdlines.txt. [GuiRunOnce], a section in the answer file, runs in the context of a user account and after the user logs on for the first time. This is an ideal place to run user specific scripts, such as scripts that add printers or scripts that automatically configure a user's e-mail configuration.

5. How does Syspart differ from Sysprep?

   Syspart is a switch of Winnt32.exe. This switch completes the Pre-Copy phase of Windows 2000 Server Setup. After it is complete, the disk used for the Pre-Copy phase can be installed in another com-puter. Upon booting from this disk, the text mode phase of setup continues. Syspart is ideal for dissimilar systems that require a faster setup procedure than is provided by running Windows 2000 Setup manually. Syspart can be further automated by calling an answer file as well as Syspart from the Winnt32 command line.

   Sysprep prepares a computer for imaging. After the operating system and applications are installed on a computer, Sysprep is run to prepare it for imaging. Next, an imaging utility is used to create an image of the prepared disk. The image is downloaded to identical or nearly identical computers, and Sysprep Mini-Setup continues to complete the installation. The Mini-Setup process can be further automated with a Sysprep.inf file.

Chapter 4

Review

1. You install a new 10-GB disk drive that you want to divide into five equal 2-GB sections. What are your options?

   You can leave the disk as a basic disk and then create a combination of primary partitions (up to three) and logical drives in an extended partition; or you can upgrade the disk to a dynamic disk and create five 2-GB simple volumes.

2. You are trying to create a striped volume on your Windows 2000 Server to improve performance. You confirm that you have enough unallocated disk space on two disks in your computer, but when you right-click an area of unallocated space on a disk, your only option is to create a partition. What is the problem, and how would you resolve it?

   You can create striped volumes on dynamic disks only. The option to create a partition rather than a volume indicates that the disk you are trying to use is a basic disk. You will need to upgrade all the disks that you want to use in your striped volume to dynamic disks before you stripe them.

3. You dual boot your computer with Windows 98 and Windows 2000. You upgrade Disk 1, which you are using to archive files, from basic storage to dynamic storage. The next time you try to access your files on Disk 1 from Windows 98, you are unable to read the files. Why?

   Only Windows 2000 is able to read dynamic storage.

4. What is the default permission when a partition is formatted with NTFS? Who has access to the volume?

   The Everyone group is granted Full Control permission. All users are members of the Everyone group, so they all have access.

   The default permission is Full Control. The Everyone group has access to the volume.

5. If a user has Write permission for a folder and is also a member of a group with Read permission for the folder, what are the user's effective permissions for the folder?

   The user has both Read permission and Write permission for the folder because NTFS permissions are cumulative.

6. What happens to permissions that are assigned to a file when the file is moved from one folder to another folder on the same NTFS partition? What happens when the file is moved to a folder on another NTFS partition?

   When the file is moved from one folder to another folder on the same NTFS partition, the file retains its permissions. When the file is moved to a folder on a different NTFS partition, the file inherits the permissions of the destination folder.

7. If an employee leaves the company, what must you do to transfer owner-ship of his or her files and folders to another employee?

   You must be logged on as Administrator to take ownership of the employee's folders and files. Assign the Take Ownership special access permission to another employee to allow that employee to take ownership of the folders and files. Notify the employee to whom you assigned Take Ownership to take ownership of the folders and files.

8. What is the best way to secure files and folders that you share on NTFS partitions?

   Put the files that you want to share in a shared folder, and keep the default shared folder permission (the Everyone group with the Full Control permission for the shared folder). Assign NTFS permissions to users and groups to control access to all contents in the shared folder or to individual files.

Chapter 5

9. Which folder represents a location on a server other than Server01? (Page 227)

   The intranet folder's physical path on Server02 is C:\inetput\wwwroot.

10. Which folder represents a mounted drive to a previously empty folder?

    The ftp folder was a previously empty folder on Server01. The empty folder path is C:\inetput\ftproot. This directory points to an extended partition on Disk0.

11. Earlier in this exercise, you created a replica of the Press Dfs link. The name of that replica is \\SERVER01\PressRepl. This Dfs link is a shared folder by the name of PressRepl and is located in C:\Public\Press. If you examine the contents of this directory, you will notice that it is empty. However, when you view the News Dfs link, you will notice that there is a file named Press.wri. Why is the PressRepl Dfs replica empty? (Page 228)

Because replication and synchronization are not supported in a stand-alone Dfs. Therefore, you must manually copy any files ap-pearing in H:\Press (the \\Server01\Press share) to the directory C:\Public\Press (the \\Server01\PressRepl share) so that \\Server01\PressRepl can serve as a replica of \\Server01\Press. Once the files are copied over, the \\Server01\Public\News Dfs link will be fault tolerant because \\Server01\PressRepl will take over if \\Server01\Press becomes unavailable.

Review

1. How does a mounted drive to an empty folder differ from a Dfs root?

   A mounted drive to an empty folder allows for folder redirection. When you store files in a folder that points to a mounted partition, the files are redirected to the partition. This feature provides limited resource consolidation. A Dfs root provides a central point where disparate resources are consolidated through Dfs links. These links are then presented to the users as a single share containing folders. This feature provides robust resource consolidation.

2. In Exercise 1, you were asked to notice that New Root Replica and Replication Policy were not available options in the Distributed File System snap-in. Explain why these options are not available.

   New Root Replica and Replication Policy are available only for domain Dfs roots. In Exercise 1 you configured a stand-alone Dfs root. A new root replica allows you to replicate the Dfs root to other servers on the network. This feature provides fault tolerance and load balancing. If a server hosting the Dfs root fails, users access the Dfs root from the other replicas. If all servers replicating the Dfs root are available, they will load balance user requests. Replication policy allows you to configure the settings for replicating the Dfs root and Dfs shares below it.

3. Why doesn't Dfs directly provide a security infrastructure?

   Security is provided by the underlying file system. A Dfs link that points to an NTFS partition is secured using NTFS permissions or share rights; a FAT partition is secured with share rights. A Dfs link to another network operating system (NOS) is secured with native security provided by the operating system. For example, NetWare provides trustee directory and file assignments for security.

A NetWare resource can be made available to Dfs through Gateway Services for NetWare.

4. How is the KCC involved in maintaining Active Directory store synchro-nization between domain controllers?

   KCC creates a ring topology for intra-domain replication. This topology provides a path for Active Directory store updates to flow from one domain controller to the next. It also provides two replica-tion paths, a path on either side of the ring to continue replication even if the ring structure is temporarily broken.

5. What data does the FRS replicate?

   System Volume data and domain Dfs roots and Dfs links configured for replication.

Chapter 6

3. Examine each of the nodes below microsoft.com. Do not modify any information that you see in these nodes.

   What selections are listed under microsoft.com and what is their purpose? Hint, choose the properties of each node in the console tree to view their purpose. (Page 276)

   Built-in – contains local groups created during installation of the domain controller.

   Computers – this is the default container for upgraded computer accounts. You can move these computers to other containers if your design requires it.

   Domain Controllers – this is the default container for new Windows 2000 domain controllers. You will see Server01 in this container.

   ForeignSecurityPrincipals – this is the default container for object SIDs from external, trusted domains. Users – this is the default container for upgraded and built-in user accounts.

4. Click the Start button, point to Programs, and then point to Administra-tive Tools.

   Notice that all installed Administrative Tools applications appear under Administrative Tools rather than just the most recently used applications.

   When Server01 was a stand-alone server, all the applications appeared under Administrative Tools except those specific to Active Directory, domain, and DNS maintenance. Using your mouse, point to each of the applications listed below to see the screen hint, and then write a descrip-tion in the space provided.

   Active Directory Domains and Trusts

   Active Directory Sites and Services

   Active Directory Users and Computers

   DNS (Page 279)

   Active Directory Domains and Trusts – manages the trust relation-ships between domains.

   Active Directory Sites and Services – creates sites to manage the replication of Active Directory data information.

   Active Directory Users and Computers – manages users, computers, security groups, and other objects in the Active Directory store.

   DNS – manages the DNS Domain Naming System (DNS) service for IP host name resolution.

Review

1. What is Ntdis.dit, and what is its purpose?

   NTDIS.DIT is the file that contains the Active Directory store.

2. What is the one SYSVOL location requirement?

   SYSVOL must be located on an NTFS 5.0 partition.

3. What is the function of SYSVOL, and what is the one disk requirement for SYSVOL?

   SYSVOL stores the domain controllers copy of the domain's public files. The contents of this directory are replicated to all domain controllers in the domain.

4. What is the difference between an attribute and an attribute value? Give examples.

   Attributes (also referred to as properties) are categories of informa-tion and define the characteristics for all objects of a defined object type. All objects of the same type have the same attributes. Values of the attributes make the objects unique. For example, all user account objects have a First Name attribute; however, the value for the First Name attribute can be any name, such as John or Jane.

5. What is the difference between modifying an object and modifying the attribute values of an object instance?

   Modifying an object is an advanced procedure completed in tools such as the Schema Manager snap-in (Schmmgmt.msc). Modifying the attribute values of an object instance involves changing data stored with an instance of an object, for example, changing the primary phone number data for a user object named John Smith.

6. You want to allow the manager of the sales department to create, modify, and delete only user accounts for sales personnel. How can you accomplish this?

   Place all the sales personnel user accounts in an OU, and then delegate control of the OU to the manager of the sales department.

7. What is the global catalog, and what is its purpose?

   The global catalog stores key information about every object in a domain tree or forest. It contains a partial replica of the Entire Directory. Only the most important data about objects are stored in the global catalog, so replicating the global catalog is more efficient than replicating the entire Active Directory store. The global catalog enables a user to find information regardless of which domain in the tree or forest contains the data.

Chapter 7

6. In what mode is the console running? (Page 315)

   The console is running in author mode as shown in the Console Mode drop-down list box.

13. When will the account expire? (Page 329)

    According to the current settings, the account will never expire. The Account Expires section at the bottom of the Account page shows that the expiration is set to Never.

5. Click OK to close the Change Password message box.

   Were you able to log on successfully? Why or why not? (Page 330)

   You were not allowed to log on locally since this right is not granted to regular user accounts. By default administrators have the right to log on locally to a domain controller, but regular users, like Jane Doe, do not.

Review

1. When you use the Administrative Tools program group to open an MMC console provided with Windows 2000 Server, can you add snap-ins to it? Why or why not?

   No, snap-ins cannot be added to the MMC consoles provided with the product when the consoles are opened from the Administrative Tools program group. These consoles are configured for User Mode operation. You can open these consoles in author mode by appending the name of the path and the name of the .msc file with MMC /a. For example:

   mmc /a %SystemRoot%\system32\compmgmt.msc /s

   opens the Computer Management console in author mode.

2. You receive a call from a member of the Help Desk support team. She tells you that a number of users are complaining of a window that appears every time they log on. The support person tells you there is nothing in the Startup menu. Additionally, she has closed the window and shut down and restarted the computer, but the window still appears at logon. What is the most likely cause of this issue, and how can you resolve it?

All the users complaining of this problem are using a mandatory shared profile. When the profile template was built, a window was left open on the desktop. To resolve this problem, make sure no users are accessing the profile, rename Ntuser.man to Ntuser.dat so that it is no longer mandatory. Log on with a user account that points to this profile, close the window that appears, and then log off. Upon logoff, the profile change will be saved to the network shared profile location. Next, rename Ntuser.dat back to Ntuser.man and instruct the users to log on again.

3. When should you use security groups instead of distribution groups?

   Use security groups to assign permissions. Use distribution groups when the only function of the group is not security related, such as an e-mail distribution list. You cannot use distribution groups to assign permissions.

4. What are the implications of changing the domain mode from Mixed mode to Native mode?

   Pre–Windows 2000 domain controllers cannot participate in a Native-mode domain.

   Pre–Windows 2000 stand-alone servers and computers running Windows NT Workstation can still participate in the domain.

   After you change to Native mode, you cannot change back to Mixed mode.

5. By default, in what order is group policy implemented through the Active Directory store hierarchy? How can you control this behavior?

   Group policy is implemented in the following order: site, domain, and then organizational unit (OU).

   You can control group policy inheritance through the Block Policy Inheritance check box. However, the No Override Link option set in higher levels of the hierarchy supersedes this option. Additionally, you can restrict who group policies are applied to by modifying the security settings for the group policy.

6. What is a GPO, GPC, and GPT?

   A GPO is a group policy object. Group Policy configuration settings are contained within a GPO. You establish group policy settings in a GPO that you apply to a site, domain, or OU. GPOs store group policy information in two locations: a GPC and a GPT.

A GPC, or group policy container, is an Active Directory object that contains GPO properties and includes subcontainers for computer and user group policy information. The GPC contains the class store information for application deployment. The Windows 2000 class store is a server-based repository for all applications, interfaces, and application programming interfaces (APIs) that provide application publishing and assigning functions.

A GPT, or group policy template, is a folder structure in the system volume folder (Sysvol) of domain controllers. The GPT is the con-tainer for all software policy, script, file and application deployment, and security settings information. The folder name of the GPT is the globally unique identifier (GUID) of the GPO you created.

Chapter 8

Review

1. Explain the difference between a print device and a printer.

   A print device is the hardware that creates printable pages or a file on a disk (print to file) that has been processed through a printer. A printer is the software interface to one or more print devices.

2. You are told by a colleague never to remove the Everyone system group from the permissions of a printer or no one will be able to manage the printer or its documents. Why is this statement incorrect? How could you configure this undesirable behavior?

   Removing the Everyone system group from a printer's permissions still leaves a number of groups (Administrators, CREATOR OWNER, Printer Operators, and Server Operators) that have access to the printers by default. Removing the Everyone system group is not the same as specifically denying the Everyone system group with access to the printer. This configuration would result in the inability to manage the printer until the deny permission is removed by the CREATOR OWNER system account.

3. You have configured two Windows 2000 print servers on your network. When a user connects to one from Windows 95, printing is automatic. When the same user connects to the same print server for a different printer, she gets prompted to install a driver. Why is this happening?

One printer installed on the print server has been configured with additional drivers, specifically the Windows 95 or 98 printer driver. The other printer has not been configured with additional drivers.

4. In an environment where many users print to the same print device, how can you help reduce the likelihood of users picking up the wrong documents?

   Create a separator page that identifies and separates printed documents.

5. Can you redirect a single document?

   No. You can change only the configuration of the print server to send documents to another printer or print device; this change redirects all documents on that printer. The currently spooled or active document cannot be redirected.

6. A user needs to print a very large document. How can the user print the job after hours without being present while the document prints?

   You can control print jobs by setting the printing time. You set the printing time for a document on the General tab of the Properties dialog box for the document. To open the Properties dialog box for a document, select the document in the Printers window, click Docu-ment on the Printers window menu bar, and then click Properties. Click Only From in the Schedule section of the Properties dialog box, and then set the Only From hour to the earliest time you want the document to begin printing after regular business hours. Set the To time to a couple of hours before normal business hours start. To set the printing time for a document, you must be the owner of the document or have the Manage Documents permission for the appro-priate printer.

Chapter 9

Review

1. Your computer receives its TCP/IP configuration information from a DHCP server in the network. After DHCP information is received, you can connect to any host on your own subnet, but you cannot connect to or successfully ping any host on a remote subnet. You checked the DHCP Service to ensure that the router information specified for your address scope is correct. What is the likely cause of the problem and how would you fix it?

The default gateway is incorrectly specified on your computer. If default gateway information is specified on a client computer, these settings take precedence over settings downloaded from a DHCP server. To solve this configuration problem, simply remove the default gateway information from the client computer and then run IPCONFIG /renew from the command line. Other possibilities are that the default gateway is offline or that the subnet mask is incorrect.

2. You installed NWLink IPX/SPX and GSNW. After installing these components, you cannot communicate with one of the NetWare servers on your network. You have no trouble accessing this NetWare server from your client computer running Windows 2000 Professional, NWLink IPX/SPX, and CSNW. You must communicate with this NetWare server from your Windows 2000 Server because the NetWare server contains resources you must make available to users running the Microsoft Network Client. What is the likely cause of the problem?

   Although the NWLink implementation in Windows 2000 can auto-matically detect a frame type for IPX/SPX-compatible protocols, it can only automatically detect one frame type. It's possible that the Windows 2000 Server detected the wrong frame type. If the network is configured for multiple frame types, you must manually configure the frame type that matches the frame type of the NetWare server you are attempting to access.

3. You notice that access to network resources seems slower on your computer running Windows 2000 Server than from another identical computer running Windows 2000 Server on the same network. The only difference you can determine is that the slower Windows 2000 Server computer is running multiple protocols. How could network protocol binding order potentially resolve this problem?

   You specify the binding order to optimize network performance. For example, a computer running Windows 2000 Server has NetBEUI, NWLink IPX/SPX, and TCP/IP installed. However, most of the servers to which this computer connects are running only TCP/IP. You would adjust the binding order so that the Workstation service binding to TCP/IP is listed before the other Workstation service bindings for the other protocols. In this way, when you attempt to connect to another computer, the Workstation service first attempts to use TCP/IP to establish the connection.

4. When do DHCP clients attempt to renew their leases?

   When 50 percent of the lease life has expired, the DHCP client attempts to renew its lease with the DHCP server that leased the address originally. If the lease isn't renewed, the DHCP client will renew its lease with any DHCP server after 87.5 percent of its cur-rent lease life has expired.

5. Why might you create multiple scopes on a DHCP server?

   You might create multiple scopes on a DHCP server to centralize administration and to assign IP addresses specific to a subnet (for example, a default gateway). You can assign only one scope to a specific subnet.

6. How can you manually restore the DHCP database?

   You can change the RestoreFlag key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DHCPServer\Parameters to 1 in the registry and then restart the DHCP Service, or you can manu-ally copy the files in the DHCP backup folder to the DHCP directory and then restart the service.

7. What are the configuration requirements for a WINS server?

   The requirements are a computer running Windows 2000 Server configured with WINS, and a static IP address, subnet mask, and default gateway.

   You can also configure a static mapping for all non-WINS clients on the WINS server, WINS support on a DHCP server, and a WINS proxy agent on WINS-enabled clients.

8. Why would you want to have multiple name servers?

   Installing multiple name servers provides redundancy, reduces the load on the server that stores the primary zone database file, and allows for faster access speed for remote locations.

9. Why do you create forward and reverse lookup zones?

   A name server must have at least one forward lookup zone. A for-ward lookup zone enables name resolution.

   A reverse lookup zone is needed for troubleshooting utilities, such as nslookup, and to record names instead of IP addresses in IIS logs.

10. What is the difference between dynamic DNS and DNS?

    Dynamic DNS allows automatic updates to the primary server's zone file. In DNS, you must manually update the file when new hosts or domains are added.

    Dynamic DNS also allows a list of authorized servers to initiate updates. This list can include secondary name servers, domain controllers, and other servers that perform network registration for clients, such as servers running WINS and the DHCP Service.

Chapter 10

Review

1. What is the purpose of demand-dial routing?

   Demand-dial routing provides a facility for connecting one dial-up router to another dial-up router. This allows two routers on separate networks to use a dial-up infrastructure such as the public switched telephone network or the Internet to connect to each other and transfer information. A two-way initiated connection allows each router to accept inbound data from an opposing router and initiate outbound data to the opposing router.

2. What authentication providers are available in RRAS and how are they different from authentication methods?

   There are two authentication providers: Windows authentication and RADIUS authentication. Windows authentication uses the Windows 2000 directory for authenticating user accounts. RADIUS authentication uses either the Microsoft IAS RADIUS server or a third-party RADIUS server to authenticate user accounts. Authenti-cation methods are a security process where by the client and the server agree on a procedure for authenticated account information. RRAS supports EAP, MS-CHAP v2, MS-CHAP, CHAP, SPAP, PAP, and clear text authentication.

3. What is the purpose of VPN and what two VPN technologies are sup-ported in Windows 2000 RRAS?

   VPN or virtual private networking provides a facility to securely transfer data over a public network. The two VPN technologies supported in Windows 2000 RRAS are PPTP and L2TP.

4. If a remote access client begins to connect to the RAS server but the connec-tion is dropped, what troubleshooting steps will help you to solve this error?

   1. **Verify that Event Logging is enabled and view the System Event log on the computer running RRAS.**
   2. **On the remote access client, access the properties of the dial-up device, such as a modem, click the Diagnostics tab, and check the Record a Log check box. After attempting a connection, review the log file.**
   3. **On the server, open the Authentication Methods dialog box and check the Allow remote systems to connect without authentica-tion check box. After selecting this check box, attempt to recon-nect from the client computer.**

5. How is the remote access permission of Deny Access (in Mixed mode or Native mode), similar in function to the Native-mode domain default remote access policy?

   The Deny Access remote access permission does not allow a user with this setting to use remote access to connect to the server. The native-mode domain remote access policy is Allow Access If Dial-In Permis-sion Is Enabled. The default policy's properties, however, are Deny Remote Access Permission At All Times.

6. You need to configure 10 RRAS servers for a client. All 10 servers will have identical RRAS configurations. What is the most efficient way to complete this configuration?

   Configure one RRAS server to act as the master configuration for all other RRAS servers. Then, use netsh to dump the configuration and then use the –f or exec command to run the script. For example, to dump the RAS configuration from a server named RRAS1 to a script file named Ras.scr, from RRAS1 type:
   netsh –c RAS dump >ras.scr

   Next, to apply this policy to a RRAS server named RRAS2 from RRAS1, type:
   netsh –r RRAS2 –f ras.scr.928

Chapter 11

Review

1. Which key is associated with the creation of digital signatures, the public key or the private key? Explain your answer.

   Private keys are associated with the creation of digital signatures. You use a private key to transform data in such a way that users are able to verify that only you could have created the encrypted data. Decrypting the data is achieved through the application of the public key. However, only the private key is used to create the digital signature.

2. What security credential(s) will be in use if you are supporting client computers running Windows 2000 and Windows NT that authenticate to servers running Windows 2000 Server, and Windows NT Server?

   Windows NT client computers will authenticate to both Windows 2000 and Windows NT Servers using NTLM credentials (Windows NT domain name, username, and encrypted password). Windows 2000 client computers will authenticate to the computers running Windows 2000 Server using Kerberos authentication (domain name, username, Kerberos encrypted password), and they will authenticate to the computers running Windows NT Server using NTLM authentication.

3. How can a security template be used to facilitate configuration and analysis of security settings?

   A template can be applied to a security configuration database created by the Security Analysis and Configuration snap-in. After the database is created, the current settings of the computer can be compared to the settings dictated by the policy. After reviewing discrepancies between policy and computer security settings, the same snap-in can be used to configure the computer's security settings to the template's settings.

4. Where is the Certificate Services Enrollment page and what is its purpose?

   The Certificate Services Enrollment page is a Web page that allows for the easy creation and monitoring of certificate requests, and for the retrieval of CRLs and certificates.

5. What steps must you follow to enable auditing of specific file objects on domain controllers in a domain where Group Policy is enabled?

   Use Active Directory Users And Computers to open a group policy (typically the Default Domain GPO or the Default Domain controller Policy GPO). Navigate to the Audit Policy node below the Windows Settings - Security Settings – Local Policies node. In the details pane, double-click Audit Object Access and enable success or failure attempts as appropriate. Using Windows Explorer, navigate to the specific file or folder that you need to access. Access the properties of the file or folder object, click the Security tab, then click the Ad-vanced button. From the Access Control Settings dialog box, select View/Edit to modify the audit policy of a selected user or group or add a new user or group to audit. Be cautious about how much file object auditing you configure. This feature can be processor inten-sive if it is configured improperly.

Chapter 12

Review

1. You have configured a computer to boot Windows 2000 Server as the default operating system, and Windows NT 4.0 Server as the optional operating system. After modifying the attributes of files on %systemdrive% and deleting some of the files, the computer does not display Windows NT 4.0 Server as an operating system to start. Windows 2000 Server starts up properly. The problem is caused because you deleted a file. What is the name of the file, and what can you do to recover from this error?

   You deleted the Boot.ini file. Boot.ini allows for multiboot. If this file is missing, the default operating system starts. To recover this file, run the ERD, choose Manual Repair, and then choose Inspect Startup Environment.

2. You have created three hardware profiles for your mobile computer: Docked, Undocked On The Network, and Undocked At Home. When you reboot the computer, the first two hardware profiles appear, but the third one does not. What is the most likely reason that the Undocked At Home profile does not appear?

In the properties of the Undocked At Home profile, the Always Include This Profile As An Option When Windows Starts check box is not selected.

3. Why would the Use Hardware Compression, If Available check box be unavailable in the Backup wizard?

   This option is available only if an installed tape device and its driver supports hardware compression.

4. You performed a normal backup on Monday. For the remaining days of the week, you only want to back up files and folders that have changed since the previous day. What backup type do you select?

   Incremental. The incremental backup type backs up changes since the last markers were set and then clears the markers. Thus, for Tuesday through Friday, you only back up changes made since the previous day.

5. How can you test the configuration of the UPS service on a computer?

   You can simulate a power failure by disconnecting the main power supply to the UPS device. During the test, the computer and periph-erals connected to the UPS device should remain operational, mes-sages should display, and events should continue to be logged.

   In addition, you should wait until the UPS battery reaches a low levelto verify that a graceful shutdown occurs. Then restore the main power to the UPS device and check the event log to ensure that all actions were logged and there were no errors.

   Note that this procedure requires a UPS that communicates with the computer through a COM port or a proprietary interface provided with the UPS.

Chapter 13

Review

1. You have used the Compact utility to compress the files contained in the Users subfolders on an NTFS partition. You have enabled the Folder Option, Display Compressed Files And Folders With Alternate Color. A week later you use Windows Explorer to see if files are being com-pressed. To your surprise, user account subfolders, located directly under the Users folder created after you ran the compress utility, are not compressed. Why did this happen and how can you fix it?

   You ran the Compact utility and compressed each of the subfolders under the Users subfolder. As a result, all subfolders were marked for compression but the Users parent folder was not marked for compression. Therefore, new folders created directly below the Users folder are not compressed. There are a number of ways to fix this. You can use the Compact utility to mark the Users folder for compression and all subfolders below users. Open a command prompt, go to the driver containing the Users parent folder, and type compact /s:Users /c. Or you can use the Windows Explorer to compress the Users subfolder and then choose the Apply changes to this folder, subfolders and files radio button.

2. Your department has recently archived several GB of data from a com-puter running Windows 2000 Server to CD-ROMs. As users have added files to the server, you have noticed that the server has been taking longer than usual to gain access to the hard disk. How can you increase disk access time for the server?

   Use Disk Defragmenter to defragment files on the server's hard disk.

3. You are the administrator for a computer running Windows 2000 Server that is used to store user's home folders and roaming user profiles. You want to restrict users to 25 MB of available storage for their home folder while monitoring, but not limiting, the disk space used for the roaming user profiles. How should you configure the volumes on the server?

Create two volumes: one to store home folders and another to store roaming user profiles. Format both volumes with NTFS, and enable disk quotas for both volumes. For the home folder volume, specify a limit of 25 MB and select the Deny Disk Space To Users Exceeding Quota Limit check box. For the roaming user profile volume, do not specify a limit and clear the Deny Disk Space To Users Exceeding Quota Limit check box.

4. You notice that a new server is not performing as well as you expected. You need to obtain summary information on a server's performance, and then you want to use a utility to obtain detailed reports of performance bottlenecks. After you have resolved the performance problem, what should you do to track the performance of the server as more users begin to access the server?

   To obtain summary information on a server's performance, run Task Manager to observe common data points contained under the Performance tab. This can give you an idea of where your perfor-mance bottleneck is. Next, run the System Monitor snap-in and observe detailed performance metrics. Add resources as necessary or remove applications that are creating the bottleneck. After you have resolved the performance issue, use the Performance Logs And Alerts to log performance activity. These logs serve as your baseline for future performance monitoring. So that you are not caught off-guard by poor performance or a potential hardware failure, create alerts to track the activity of the server. If you think poor perfor-mance might be related to network activity, run the Network Moni-tor to analyze network activity.

5. You want to filter out all network traffic except for traffic between two computers, and you also want to locate specific data within the packets. Which Network Monitor filter features should you specify?

   Filter for Address Pairs where you specify the media access control address of each computer, and then specify Pattern Matches where you filter for specific patterns in Hex or ASCII contained in the frames.

6. You goal is to make sure that only two network management stations in your organization are able to communicate with the SNMP agents. What mea-sures can you take when configuring the SNMP service to enhance security?

Using the Security tab of the SNMP Service Properties dialog box, make the following configuration changes:

- **Specify a unique community name and remove the public community name.**
- **Adjust the community rights settings so that the NMS can complete the functions you want to enable. If you aren't sure of the community rights you need, configure this for READ ONLY and adjust it by NMS to SNMP service testing.**
- **Select the Accept SNMP packets from these hosts radio button, and then specify the host name, IP, or IPX address of the two network management stations.**
- **If you will be sending Traps to an NMS, make sure to specify the Trap destination(s) under the Traps tab.**

Chapter 14

7. With the Web Site tab active, record the TCP Port value appearing in the TCP Port text box.

   Port value will vary but should be between 2000-9999.

Review

1. Compare a virtual directory to a Dfs root.

   A virtual directory is a term used to describe Web server directories that appear to be located below a Web server's home directory but could be located in any location accessible to the Web server. An alias is used to describe the virtual directory so that Web browser users are unaware of the virtual directories' physical location or path.

   A Dfs root is also a symbolic share that provides centralized access to shares located throughout the network. The user is unaware of the physical location of the shares but is able to reach them by starting from the Dfs root. The Dfs root is similar to an Internet Information Services (IIS) home directory and the shares below the Dfs root are similar to virtual directories in IIS.

2. You are accessing the IIS 5.0 documentation from Internet Services Manager (HTML). All of the documentation appears and you are able to access information via the Index tab. Under the Index tab, you find the phrase Process Accounting. However, when you perform a search on this phrase, the Web browser reports that your search phrase cannot be found. What is the most likely reason that this is happening?

   The indexing service has been started since the Web browser did not report the inability to perform a search. Because the phrase was not found it could be that you have not configured the Indexing Service to catalog the iisHelp folder or the Indexing Service has not com-pleted the task of indexing this folder's contents.

3. You have created a virtual directory for the purpose of WebDAV publish-ing. The home directory of the Web site is accessible from Internet Explorer 5, but when you attempt to access the virtual directory for WebDAV publishing, access is denied. Name two reasons why this may happen and how you can solve this access problem.

   WebDAV security is managed by the file system and Internet Ser-vices. Therefore, access could be denied because the physical direc-tory for WebDAV has an ACL that does not allow the browser client to access the folder. If access is allowed at the file system level, verify that Read, Write, and Directory Browsing on the WebDAV virtual directory is enabled. For ASP support also make sure to enable Script source access.

4. Why is it important that the Microsoft Telnet Client and the Microsoft Telnet service support NTLM authentication?

   NTLM authentication protects authentication information from being transmitted across a network from the Telnet client to the Telnet server. A user is authenticated in the context of the current logon. If authentication is necessary, NTLM challenge/response authentication protects logon information. This is an important security feature of Windows 2000 Telnet.

5. If Terminal Services is not licensed, what features of Terminal Services will work and for how long?

   Remote Administration mode allows for two remote control sessions with the computer running Terminal Services. No Terminal Service client license is necessary for this function. In Application Server mode, a Terminal Service client license is required for each session. The Terminal Service will continue to function for 90 days without Terminal Service client licenses installed on the Terminal Services License server.

Appendix B

Sample Answer Files for Unattended Setup

Unattended Setup in Microsoft Windows 2000 uses an ASCII text file that is called an answer file to supply data that would otherwise be entered interactively when you run the Setup wizard.The answer file is specified on either a Winnt.exe or Winnt32.exe command line when the Unattended Setup option is used.

This appendix includes sample answer files that are appropriate for common installation configurations.You can customize the default answer file (Unattend.txt) that comes with Windows 2000 or write a new one based on the samples that are provided in this appendix.

In This Appendix

- Answer file format
- Sample answer files

Answer File Format

An answer file consists of section headers, keys, and the values for each key. Most of the section headers are predefined, but some can be user defined. You do not need to specify all the possible keys in an answer file if the installation does not require them.Invalid key values generate errors or can cause incorrect behavior after setup.The file format is as follows:

[section_name]

Sections contain keys and the corresponding values for those keys. Each key and value are separated by a space, an equal sign, and a space.The following is an example:

key = value

Values that have spaces in them require double quotes around them. The following is an example:

key = "value with spaces "

Some sections have no keys and merely contain a list of values.The following is an example:

[OEMBootFiles]
Txtsetup.oem

Comment lines start with a semicolon.

;This is an example of a comment line.

Answer File Keys and Values

Every key in an answer file must have a value assigned to it; however, some keys are optional, and some keys have default values that are used if the keyis omitted.

Key values are strings of text unless numeric is specified. If numeric is specified, the value is decimal unless otherwise noted.

Note Keys are not case sensitive;they can be uppercase or lowercase.

The Unattend.doc file has detailed information about the answer file keys andvalues. To find this file, look on the Windows 2000 installation CD-ROM in the \Support \Tools folder for Deploy.cab.To extract or view the contents of the Deploy.cab file, use Windows Explorer.

Sample Answer Files

The sample answer files that are provided in this section are examples of the more common installation configurations of the keys commonly used in those configurations. Consider these files as examples only, and modify them as appropriate for your organization.

Note In the answer files that follow, the use of italic font style indicates that the user must supply the required information.

Sample 1 – Default Unattend.txt.

The following answer file is the default Unattend.txt file provided on the Windows 2000 CD.

```
;Microsoft Windows 2000 Professional, Server, Advanced Server and
Datacenter
;(c)1994 -1999 Microsoft Corporation.All rights re- served.
;
;Sample Unattended Setup Answer File
;
;This file contains information about how to automate the installation
;or upgrade of Windows 2000 Professional and Windows 2000 Server so the
;Setup program runs without requiring user input.
;

[Unattended]
Unattendmode = FullUnattended
OemPreinstall = NO
TargetPath = WINNT
Filesystem = LeaveAlone

[UserData]
FullName = "Your User Name"
OrgName = "Your Organization Name"
ComputerName ="COMPUTER_NAME"

[GuiUnattended]
;Sets the Timezone to the Pacific Northwest
;Sets the Admin Password to NULL
;Turn AutoLogon ON and login once
TimeZone = "004 "
```

```
AdminPassword = *
AutoLogon = Yes
AutoLogonCount = 1.
;For Server installs
[LicenseFilePrintData]
AutoMode = "PerServer "
AutoUsers = "5 "

[GuiRunOnce]
;List the programs that you want to lauch when the machine is logged into for
the first time

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 70

[Networking]
;When set to YES, setup will install default networking components.The
components to be set are
;TCP/IP, File and Print Sharing, and the Client for Microsoft Networks.
Install Default Components = YES
[Identification]
JoinWorkgroup = Workgroup
```

Sample 2 – Unattended Installation of Windows 2000 Professional from CD-ROM

The following answer file installs Microsoft Windows 2000 Professional from CD-ROM. For this answer file to function properly, you must name it Winnt.sif and place it on a floppy disk.

```
;Microsoft Windows 2000 Professional
;© 1994 –1999 Microsoft Corporation.All rights reserved.
;
;Sample Answer File for Unattended Setup
;
;This file contains information about how to automate the installation
;or upgrade of Windows 2000 Professional so that the Setup program runs
;without requiring user input.
;
```

[Data]
;This section is required when you perform an unattended installation
;by starting Setup directly from the Windows 2000 installa- tion CD-ROM.
Unattendedinstall = Yes
;If you are running Unattended Setup from the CD-ROM, you. must set the
;Msdosinitiated key to 0. Msdosinitiated = "0 "
;AutoPartition allows Windows 2000 Unattended Setup to choose a
;partition to install to. AutoPartition = 1

[Unattended]
UnattendMode = FullUnattended
;The OemPreinstall key tells Unattended Setup that the installation is
;being performed from distribution shares if the value is set to Yes.
OemPreinstall = Yes
TargetPath = Winpro
FileSystem = LeaveAlone
;If the OemSkipEula key is set to Yes, it informs Unat- tended Setup that
;the user should not be prompted to accept the End User License
;Agreement (EULA).A value of Yes signifies agreement to the EULA and
;should be used in conjunction with the terms of your license
;agreement.
OemSkipEula = Yes

[GuiUnattended]
;Sets the TimeZone.For example, to set the TimeZone for the Pacific
Northwest, use a
;value of "004." Be sure to use the numeric value that represents your own
time zone.To look up
;a numeric value, see the Unattend.doc file on the Win- dows 2000 CD.
TimeZone ="*YourTimeZone*"
;It is recommended that you change the administrator pass- word before the
computer
;is placed at it 's final destination.
AdminPassword =adminpassword
;Tells Unattended Setup to turn AutoLogon ON and log on once.
AutoLogon = Yes
AutoLogonCount = 1
;The OemSkipWelcome key specifies whether the welcome page in the
;wizard phase of Setup should be skipped.A value of 1 causes the page
;to be skipped.

```
OemSkipWelcome = 1
;The OemSkipRegional key allows Unattended Setup to skip RegionalSettings.
;when the final location of the computer is unknown.
OemSkipRegional = 1

[UserData]
FullName ="Your user name"
OrgName ="Your organization name"
;It is recommended that you avoid using spaces in the  ComputerName value.
ComputerName ="YourComputer_name"
;To ensure a fully unattended installation, you must pro-  vide a value
;for the ProductId key.
ProductId ="Your product ID"

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 60

[Networking]
;When you set the value of the InstallDefaultComponents key  to Yes, Setup
will install
;default networking components.The components to be set are  TCP/IP, File
and Print Sharing,
;and the Client for Microsoft Networks.
InstallDefaultComponents = Yes
```

Sample 3 – Install and Configure Windows 2000 and Configure Microsoft Internet Explorer with Proxy Settings

The following answer file installs and configures Microsoft Internet Explorer and configures proxy settings.

```
;Microsoft Windows 2000 Professional, Server, Advanced Server
;© 1994 – 1999 Microsoft Corporation.All rights reserved.
;
;Sample Answer File for Unattended Setup
;
;This file contains information about how to automate the  installation
```

;or upgrade of Windows 2000 Professional and Windows 2000 Server so ;that the Setup program runs without requiring user input.

[Unattended]
UnattendMode = FullUnattended
TargetPath = Windows
FileSystem = LeaveAlone.
OemPreinstall = Yes
OemSkipEula = Yes

[GuiUnattended]
;Sets the TimeZone.For example, to set the TimeZone for the Pacific Northwest, use a
;value of "004." Be sure to use the numeric value that represents your own time zone.To look up
;a numeric value, see the Unattend.doc file on the Win- dows 2000 CD.
TimeZone ="*YourTimeZone*"
;It is recommended that you change the administrator pass- word before the computer
;is placed at it 's final destination.
AdminPassword = adminpassword
;Tells Unattended Setup to turn AutoLogon ON and log on once.
AutoLogon = Yes
AutoLogonCount = 1
OemSkipWelcome = 1
;The OemSkipRegional key allows Unattended Setup to skip RegionalSettings
;when the final location of the computer is unknown.
OemSkipRegional = 1

[UserData]
FullName = "*Your user name*"
OrgName = "*Your organization name*"
;It is recommended that the use of spaces be avoided in the ComputerName value.
ComputerName = "YourComputername"
;To ensure a fully unattended installation, you must pro- vide a value
;for the ProductId key.
ProductId = "Your product ID"

```
[LicenseFilePrintData]
;This section is used for server installs.
AutoMode ="PerServer"
AutoUsers = "50"

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 60

[Components]
;This section contains keys for installing the components of Windows 2000.
;A value of On installs the components, and a value of Off prevents the.
;component from being installed.
iis_common = On
iis_inetmgr = Off
iis_www = Off
iis_ftp = Off
iis_htmla = Off
iis_doc = Off
iis_pwmgr = Off
iis_smtp = On
iis_smtp_docs = Off
Mts_core = On
;The Fp key installs Front Page Server Extensions.
Fp = On
Msmq = Off
;If you set the TSEnable key to On, Terminal Services is installed on
;Windows 2000 Server.
TSEnable = On
;If you set the TSClients key to On, the files required to create
;Terminal Services client disks are installed.If you set this key to On, you must
also set the
;TSEnable key to On.
TSClients = On
;TSPrinterDrivers and TSKeyboardDrivers are optional keys.
If enabled,
;they require additional disk space.
TSPrinterDrivers = Off
```

TSKeyboardDrivers = Off
Netoc = On
Reminst = On
Certsrv = Off
Rstorage = Off
Indexsrv_system = On
Certsrv_client = Off
Certsrv_server = Off
Certsrv_doc = Off
Accessopt = On
Calc = On
Cdplayer = On
Charmap = On
Chat = Off
Clipbook = On
Deskpaper = On
Dialer = On
Freecell = Off
Hypertrm = On
Media_blindnoisy = On
Media_blindquiet = On
Media_clips = On
Media_jungle = On
Media_musica = On.
Media_robotz = On
Media_utopia = On
Minesweeper = Off
Mousepoint = Off
Mplay = On
Mswordpad = On
Objectpkg = On
Paint = On
Pinball = Off
Rec = On
Solitaire = Off
Templates = On
Vol = On

[TapiLocation]
CountryCode = "1"
Dialing = Pulse
:Indicates the area code for your telephone.This value should be a 3-digit number.
AreaCode ="*Your telephone area code*"
LongDistanceAccess = 9

[Networking]
;When you set the value of the InstallDefaultComponents key to Yes, Setup will install
;default networking components.The components to be set are TCP/IP, File and Print Sharing,
;and the Client for Microsoft Networks.
InstallDefaultComponents = Yes

[Identification]
JoinDomain = *YourCorpNet*
DomainAdmin = *YourCorpAdmin*
DomainAdminPassword = *YourAdminPassword*

[NetOptionalComponents]
;This section contains a list of the optional network components to install.
Wins = Off
Dns = Off
Dhcpserver = Off
ils = Off
Snmp = Off
Lpdsvc = Off
Simptcp = Off
Netmontools = On
Dsmigrat = Off

[Branding]
;This section brands Microsoft Internet Explorer with custom
;properties from the Unattended answer file.
BrandIEUsingUnattended =Yes.

[URL]
;This section contains custom URL settings for Microsoft Internet Explorer.If these settings
;are not present, the default settings are used.
;Specifies the URL for the browser 's default home page.For example,
;you might use:Home_Page = www.microsoft.com.
Home_Page = *YourHomePageURL*
;Specifies the URL for the default search page. For example, you might
;use:Search Page = www.msn.com
Search_Page = *YourSearchPageURL*
;Specifies a shortcut name in the link folder of Favorites.
For example,
;you might use:Quick_Link_1_Name = "Microsoft Product Support Services"
Quick_Link_1_Name = "*Your Quick Link Name*"
;Specifies a shortcut URL in the link folder of Favorites.
For example,
;you might use:Quick_Link_1 = http://
support.microsoft.com/.
Quick_Link_1 = *YourQuickLinkURL*

[Proxy]
;This section contains custom proxy settings for Microsoft Internet Explorer.If these settings are
;not present, the default settings are used.If proxysrv:80 is not accurate for yourconfiguration,
;be sure to replace the proxy server and port number with your own parameters.
HTTP_Proxy_Server = *proxysrv:80*
Use_Same_Proxy = 1
Proxy_Enable = 1
Proxy_Override = <local>

Sample 4 – Install and Configure Windows 2000 Server with Two Network Adapters

The following answer file installs Microsoft Windows 2000 Server with two network adapters;one adapter uses Dynamic Host Configuration Protocol (DHCP), and the other uses static information.

;Microsoft Windows 2000 Server, Advanced Server
;© 1994 –1999 Microsoft Corporation.All rights reserved.
;

```
;Sample Answer File for Unattended Setup
;
;This file contains information about how to automate the installation
;or upgrade of Windows 2000 Server or Windows 2000 Advanced. Server so
that
;that the Setup program runs without requiring user input.
;

[Unattended]
UnattendMode = FullUnattended
TargetPath = Winnt
Filesystem = ConvertNTFS

[GuiUnattended]
;Sets the TimeZone.For example, to set the TimeZone for the Pacific
Northwest, use a
;value of "004." Be sure to use the numeric value that represents your own
time zone.To look up
;a numeric value, see the Unattend.doc file on the Win- dows 2000 CD.
TimeZone ="YourTimeZone"
;It is recommended that you change the administrator password before the
computer
;is placed at it's final destination.
AdminPassword = adminpassword
;Tells Unattended Setup to turn AutoLogon ON and log on once.
AutoLogon = Yes
AutoLogonCount = 1

[LicenseFilePrintData]
;This section is used for server installs.
AutoMode = "PerServer"
AutoUsers = "50"

[UserData]
FullName = "Your user name"
OrgName = "Your organization name"
;It is recommended that you avoid the use of spaces in the ComputerName
value.
ComputerName = "YourComputer_name"
```

;To ensure a fully unattended installation, you must provide a value ;for the ProductId key.
ProductId = "*Your product ID*"

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 70

[Networking]
;When you set the value of the InstallDefaultComponents key to Yes, Setup will install
;default networking components.The components to be set are. TCP/IP, File and Print Sharing,
;and the Client for Microsoft Networks.
InstallDefaultComponents = Yes

[Identification]
JoinDomain = *YourCorpNet*
DomainAdmin = *YourCorpAdmin*
DomainAdminPassword = *YourAdminPassword*

[NetAdapters]
;In this example, there are two network adapters, Adapter01 and Adapter02.
;Note that the adapter specified here as 01 is not always local area network (LAN)
;connection 1 in the user interface.
Adapter01 = Params.Adapter01
Adapter02 = Params.Adapter02

[Params.Adapter01]
;Specifies which adapter is number one.
;Note that the InfID key must match a valid PNP ID in the system. For example, a valid PNP ID
;might look as follows:InfID = "pci \ven_0e11&dev_ae32"
InfID = "*Your_PNP_ID_for_Adapter01*"

```
[Params.Adapter02]
;Specifies which adapter is number two.
;Note that the InfID key must match a valid PNP ID in the system.For
example, a valid PNP ID
;might look as follows:InfID =
"pci \ven_8086&dev_1229&subsys_00018086"
InfID = "Your_PNP_ID_for_Adapter02"

[NetClients]
;Installs the Client for Microsoft Networks.
MS_MSClient = params.MS_MSClient

[Params.MS_MSClient]

[NetProtocols]
;Installs only the TCP/IP protocol.
MS_TCPIP = params.MS_TCPIP

[params.MS_TCPIP]
;This section configures the TCP/IP properties.
AdapterSections =
Params.MS_TCPIP.Adapter01, params.MS_TCPIP. Adapter02

[Params.MS_TCPIP.Adapter01]
;Adapter01 uses DHCP server information.
SpecificTo =Adapter01.
DHCP = Yes
Wins = Yes

[Params.MS_TCPIP.Adapter02]
;Adapter02 uses static TCP/IP configuration.
SpecificTo = Adapter02
IPAddress = 1.1.1.1
SubnetMask = 255.255.248.0
DefaultGateway = 2.2.2.2
DHCP = No
Wins = No
```

```
[NetServices]
;Install File and Print services.
MS_Server = Params.MS_Server

[Params.MS_Server]
```

Sample 5 – Install Windows 2000 Advanced Server with Network Load Balancing

The following answer file installs Microsoft Windows 2000 Advanced Server with Network Load Balancing.

```
;Microsoft Windows 2000 Advanced Server
;© 1994 –1999 Microsoft Corporation.All rights reserved.
;
;Sample Answer File for Unattended Setup
;
;This file contains information about how to automate the installation
;or upgrade of Windows 2000 Advanced Server so that the ;Setup program
runs without requiring user input.
;

[Unattended]
UnattendMode = FullUnattended
TargetPath = Windows
FileSystem = ConvertNTFS

[GuiUnattended]
;Sets the TimeZone.For example, to set the TimeZone for the Pacific
Northwest, use a
;value of "004." Be sure to use the numeric value that represents your own
time zone.To look up
;a numeric value, see the Unattend.doc file on the Windows 2000 CD.
TimeZone = "YourTimeZone"
;It is recommended that you change the administrator password before the
computer
;is placed at it 's final destination.
AdminPassword = adminpassword
;Tells Unattended Setup to turn AutoLogon ON and log on once.
AutoLogon = Yes
AutoLogonCount = 1
```

AdvServerType =Servernt

[LicenseFilePrintData]
;This section is used for server installs.
AutoMode = "PerServer "
AutoUsers = "50 "

[UserData]
FullName = "*Your user name*"
OrgName = "*Your organization name*"
;It is recommended that you avoid the use of spaces in the ComputerName value.
ComputerName = "*YourComputer_name*"
;To ensure a fully unattended installation; you must provide a value
;for the ProductId key.
ProductId = "*Your product ID*"

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 70

[Networking]
;When you set the value of the InstallDefaultComponents key to Yes, Setup will install
;default networking components.The components to be set are TCP/IP, File and Print Sharing,
;and the Client for Microsoft Networks.
InstallDefaultComponents= Yes

[Identification]
JoinDomain = *YourCorpNet*
DomainAdmin = *YourCorpAdmin*
DomainAdminPassword = *Your AdminPassword*

[NetAdapters]
;In this example, there are two network adapters, Adapter01 and Adapter02.
;Note that the adapter specified here as 01 is not always local area network (LAN)

```
;connection 1 in the user interface.The network adapters in this example are
;not identical.
Adapter01 = Params.Adapter01
Adapter02 = Params.Adapter02.

[NetBindings]
Enable = MS_WLBS, Adapter01
Enable = MS_TCPIP, Adapter02

[Params.Adapter01]
;Specifies which adapter is number one.
PseudoAdapter = No
PreUpgradeInstance = E100B1
;Note that the InfID key must match a valid PNP ID in the system.For
example, a valid PNP ID
;might look as follows: InfID = PCI \VEN_8086&DEV_1229.
InfID = Your_PNP_ID_for_Adapter01
BusType = PCI
;The ConnectionName key specifies the name for the network connection
;associated with the network adapter that you are installing.
ConnectionName = "Connection1"

[Params.Adapter02]
;Specifies which adapter is number two.
PseudoAdapter = No
PreUpgradeInstance = El90x2
;Note that the InfID key must match a valid PNP ID in the system.For
example, a valid PNP ID
;might look as follows:InfID = PCI \VEN_10b7&DEV_9050
InfID = Your_PNP_ID_for_Adapter02
BusType = PCI
;The ConnectionName key specifies the name for the network connection
associated with the
;network adapter that you are installing.
ConnectionName = "Connection2 "

[NetProtocols]
MS_TCPIP = Params. MS_TCPIP
MS_NetMon = Params. MS_NetMon
```

[Params.MS_TCPIP]
AdapterSections =
params.MS_TCPIP.Adapter01, params. MS_TCPIP.Adapter02

[Params.MS_TCPIP.Adapter01]
SpecificTo = Adapter01
DNSServerSearchOrder = 192.31.56.150
Wins = Yes
WinsServerList = 192.31.56.150
NetBIOSOptions = 0
DHCP = No
IPAddress = 192.31.56.90, 192.31.56.91
SubnetMask = 255.255.255.0, 255.255.255.0
DefaultGateway =192.31.56.150.

[Params.MS_TCPIP.Adapter02]
SpecificTo = Adapter02
DNSServerSearchOrder = 192.31.56.150
Wins = Yes
WinsServerList = 192.31.56.150
NetBIOSOptions = 0
DHCP = No
IPAddress = 192.31.56.92
SubnetMask = 255.255.255.0
DefaultGateway = 192.31.56.150

[Params.MS_NetMon]

[Params.MS_WLBS]
;This section contains keys specific to setting the properties of Network Load Balancing.
HostPriority = 1
ClusterModeOnStart = 0
ClusterIPAddress = 192.31.56.91
ClusterNetworkMask = 255.255.255.0
DedicatedIPAddress = 192.31.56.90
DedicatedNetworkMask = 255.255.255.0
ClusterName = *cluster.yourcompany.com*
MulticastSupportEnable = 0
MaskSourceMAC = 1

```
RemoteControlCode = 0x00000000
RemoteControlUDPPort = 2504
RemoteControlEnabled = 1
Ports =
80, 80, Both, Multiple, None, Equal, 443, 443, Both, Multiple, Single, Equal
AliveMsgPeriod = 2000
AliveMsgTolerance = 10
NumActions = 50
NumPackets = 100
NumAliveMsgs = 10
DescriptorsPerAlloc = 512
MaxDescriptorAllocs = 512
ConnectionCleanupDelay = 300000
NBTSupportEnable = 1

[NetClients]
MS_MSClient = Params.MS_Client

[Params.MS_Client]

[NetServices]
MS_Server =Params.MS_Server
MS_WLBS =Params.MS_WLBS

[Params.MS_Server]
Optimizations = Balance

[NetOptionalComponents]
Netmontools = 1.
```

Sample 6 – Install Windows 2000 Advanced Server with Windows Clustering

The following answer file installs Windows 2000 Advanced Server with Windows Clustering.

```
;Microsoft Windows 2000 Advanced Server.
;© 1994 –1999 Microsoft Corporation.All rights reserved.
;
;Sample Answer File for Unattended Setup
;
```

```
;This file contains information about how to automate the installation
;or upgrade of Windows 2000 Advanced Server so that the Setup program
;runs without requiring user input.
;

[Unattended]
UnattendMode = FullUnattended
TargetPath = Advsrv
FileSystem = ConvertNTFS
OemPreinstall = Yes
OemSkipEula = Yes

[GuiUnattended]
;Sets the TimeZone.For example, to set the TimeZone for the Pacific
Northwest, use a
;value of "004." Be sure to use the numeric value that represents your own
time zone.To look up
;a numeric value, see the Unattend.doc file on the Windows 2000 CD.
TimeZone = "YourTimeZone"
;It is recommended that you change the administrator password before the
computer
;is placed at it's final destination.
AdminPassword = adminpassword
;Tells Unattended Setup to turn AutoLogon ON and log on once.
AutoLogon = Yes
AutoLogonCount = 1
AdvServerType = Servernt
OemSkipWelcome = 1
;The OemSkipRegional key allows Unattended Setup to skip RegionalSettings
;when the final location of the computer is unknown.
OemSkipRegional = 1

[LicenseFilePrintData]
;This section is used for server installs.
AutoMode = "PerServer"
AutoUsers = "50 "

[UserData]
FullName = "Your user name"
OrgName = "Your organization name"
```

;It is recommended that you avoid the use of spaces in the ComputerName value.
ComputerName = "*YourComputer_name*"
;To ensure a fully unattended installation, you must provide a value for the ProductId key.
ProductId = "*Your product ID*"

[Display]
BitsPerPel = 8
XResolution = 800
YResolution = 600
VRefresh = 70

[Networking]
;When you set the value of the InstallDefaultComponents key to Yes, Setup will install
;default networking components.The components to be set are TCP/IP, File and Print Sharing,
;and the Client for Microsoft Networks.
InstallDefaultComponents = Yes

[Identification]
JoinDomain = *YourCorpNet*
DomainAdmin = *YourCorpAdmin*
DomainAdminPassword = *YourAdminPassword*

[NetAdapters]
;In this example there are three network adapters,
Adapter 01, Adapter 02,
;and Adapter 03.The adapter specified here as 01 is not always
;LAN connection 1 in the user interface.The network adapters in this example are
;not identical.
Adapter01 = Params.Adapter01
Adapter02 = Params.Adapter02
Adapter03 = Params.Adapter03

[Params.Adapter01]
;Specifies which adapter is number one.
;Note that the NetCardAddress key must match a valid address of the adapter in the system.For
;example, a valid address might look like the following:
NetCardAddress = 0x00C04F778A5A
NetCardAddress = *YourNetCardAddress*
;The ConnectionName key specifies the name for the network connection associated with
;the network adapter that you are installing.
ConnectionName = *CorpNet*.

[Params.Adapter02]
;Specifies which adapter is number two.
;Note that the NetCardAddress key must match a valid address of the adapter in the system.For
;example, a valid address might look like the following:
NetCardAddress = 0x00C04F778A5A
NetCardAddress = *YourNetCardAddress*
;The ConnectionName key specifies the name for the network connection associated with
;the network adapter that you are installing.
ConnectionName = *VendorNet*

[Params.Adapter03]
;Specifies which adapter is number three.
;Note that the NetCardAddress key must match a valid address of the adapter in the system.For
;example, a valid address might look like the following:
NetCardAddress = 0x00C04F778A5A
NetCardAddress = *YourNetCardAddress*
;The ConnectionName key specifies the name for the network connection
;associated with the network adapter that you are installing.
ConnectionName = *PrivateNet*

[NetClients]
;Installs the Client for Microsoft Networks.
MS_MSClient = Params.MS_MSClient

[Params.MS_MSClient]

```
[NetProtocols]
;Installs only the TCP/IP protocol.
MS_TCPIP =Params.MS_TCPIP

[Params.MS_TCPIP]
;This section configures TCP/IP properties.
AdapterSections =
Params.MS_TCPIP. Adapter01, params.MS_TCPIP. Adapter02,
params.MS_TCPIP. Adapter03

[Params.MS_TCPIP.Adapter01]
;CorpNet on Adapter01 uses DHCP server information.
SpecificTo = Adapter01
DHCP = Yes
DNSServerSearchOrder = 172.31.240.226, 172.31.240.225
DNSSuffixSearchOrder = CorpNet, dns.yourcompany.com
DNSDomain = CorpNet

[Params.MS_TCPIP.Adapter02]
;VendorNet on Adapter02 uses local DHCP information.
SpecificTo = Adapter02
DHCP = Yes.

[Params.MS_TCPIP.Adapter03]
;PrivateNet on Adapter03 uses static information.
SpecificTo = Adapter03
DHCP = No
WINS = No
IPAddress = 10.2.0.41
SubnetMask = 255.255.0.0
DefaultGateway = 2.2.2.2
DNSServerSearchOrder = 10.2.0.253, 10.2.0.254

[NetServices]
;Installs File and Print services.
MS_Server =Params.MS_Server

[Params.MS_Server]
```

[Components]
;Installs Windows Clustering and Administration components on
;Advanced Server when you set the value to On.
Cluster = On

[Cluster]
Name = *CorpCluster*
Action = Form
Account = *CorpAdmin*
Domain = *CorpNet*
IPAddr = 172.31.240.227
Subnet = 255.255.248.0
Network = *CorpNet, ALL*
Network = *VendorNet, ALL*

[GuiRunOnce]
;You can automate the running of Cluscfg.exe by placing Cluscfg.exe in the
[GuiRunOnce]
;section of the Unattended answer file.This executes Cluscfg.exe and
configures
;clustering on the first startup after GUI mode Setup has completed.
;You must include the full path to the program between the quotes.
"*%Windir%|Cluster |Cluscfg.exe – unattend*"

[NetOptionalComponents]
NETMONTOOLS = 1

Appendix C

Installing Service Packs

Windows 2000 makes it easier for administrators to add service packs. With older operating systems service packs had to be installed separately, after the operating system had been installed. Windows 2000 supports service pack slipstreaming, which means that the service pack is added directly to the operating system's distribution share during installation.

Windows 2000 also eliminates the need to reinstall components that were applied before a service pack was installed. This makes it much easier to install service packs on existing systems. In the past, when service packs were applied, many previously installed components had to be reinstalled. For example, when a service pack is applied to Windows NT 4.0, services such as IPX or RAS (that had been installed previously) have to be reinstalled. To address the problems that existed with Windows NT 4.0 service packs, Windows 2000 provides service pack slipstreaming and post-setup installation of service packs.

Service Pack Slipstreaming

Service pack slipstreaming refers to a service pack being integrated with an updated version of Windows 2000 on a CD-ROM or on a network share. When Windows 2000 is installed from either source, the appropriate files from the service pack are installed without having to manually apply the service pack after the installation.

To apply a new service pack, you will have to use the update.exe with the /slip switch; this will copy the updated service pack files over the existing Windows 2000 files. Some of the key files that will be replaced include the following:

- New layout.inf, dosnet.inf, and txtsetup.sif with updated checksums for all the service pack files. These files will need additional entries if any additional files have been added.
- A new driver.cab if the drivers in the cabinet file have been changed.

Post-Setup Installation of a Service Pack

A service pack is applied on an existing Windows 2000 system by running update.exe and updating the system to Windows 2000 plus the service pack. When the system state changes (adding or removing services), this tells the base system that a service pack was installed, what files were replaced or updated by the service pack, and where to install the service pack from. This means that the right files are copied from the service pack install location (network share, CD-ROM, Web site) and the right files are copied from the Windows 2000 installation source (network share or CD-ROM). This eliminates the need to reapply a service pack once the system state has changed.

Once the service pack has been applied, if the system state changes (for example, adding RAS after the service pack is applied), Windows 2000 installs the correct files, whether those files originate from the Windows 2000 CD-ROM or from the service pack. The eliminates the need to re-apply the service pack whenever the system state changes.

Glossary

5-4-3 rule A rule that states that a thinnet network can combine as many as five cable segments connected by four repeaters. How-ever, only three segments can have stations attached, which leaves two segments untapped.

10Base2 Ethernet topology that transmits at 10 Mbps over a baseband wire, and can carry a signal 185 meters. *See also* thinnet.

10Base5 *See* standard Ethernet.

10BaseFL An Ethernet network that typi-cally uses fiber-optic cable to connect computers and repeaters.

10BaseT A 10 Mbps Ethernet network topology that typically uses unshielded twisted-pair (UTP) cable to connect comput-ers. The maximum length of a 10BaseT segment is 100 meters (328 feet).

100BaseX Ethernet *See* Fast Ethernet.

100VG (Voice Grade) AnyLAN (100VGAnyLAN) An emerging networking technology that combines elements of both Ethernet and Token Ring.

A

access method The set of rules that defines how a computer puts data onto the network cable and takes data from the cable. When data is moving on the network, access methods help to regulate the flow of network traffic.

access permissions Features that control access to sharing in Windows NT Server. Permissions can be set for the following access levels: No Access—Prevents access to the shared directory, its subdirectories, and its files. Read—Allows viewing of file and subdirectory names, changing to a shared directory's subdirectory, viewing data in files, and running applications. Change— Allows viewing of file and subdirectory names, changing to a shared directory's subdirectories, viewing data in files and running application files, adding files and subdirectories to a shared directory, chang-ing data in files, and deleting subdirectories and files. Full Control—Includes the same permissions as Change,

plus changing permissions (taking ownership of the Win-dows NT file system [NTFS] files and directories only).

account *See* user account.

account lockout A Windows 2000 security feature that locks a user account if a number of failed logon attempts occur within a specified amount of time, based on security policy lockout settings. Locked accounts cannot log on.

account policy Controls how passwords must be used by all user accounts in a domain or in an individual computer.

Active Directory services The directory service included with Windows 2000 Server. It stores information about objects on a network and makes this information available to users and network administrators. Active Directory services allows users to use a single logon process to access permitted resources anywhere on the network. Active Directory services provides network admin-istrators with an intuitive hierarchical view of the network and a single point of adminis-tration for all network objects.

Address Resolution Protocol (ARP) Deter-mines hardware addresses (MAC addresses) that correspond to an IP address.

ADSL *See* Asymmetric Digital Subscriber Line (ADSL).

advanced cable testers Cable testers that work beyond the physical layer of the OSI reference model up into layers 2, 3, and even 4. They can display information about the condition of the physical cable as well as message-frame counts, excess collisions, late collisions, error-frame counts, congestion errors, and beaconing. These testers can monitor overall network traffic, certain kinds of error situations, and traffic to and from a particular computer. They indicate if a particular cable or network interface card (NIC) is causing problems.

advanced program-to-program communication (APPC) A specification developed as part of IBM's SNA (Systems Network Architecture) model and designed to enable application programs running on different computers to communicate and exchange data directly. *See also* Systems Network Architecture.

AFP *See* AppleTalk filing protocol (AFP).

agent A program that performs a back-ground task for a user and reports to the user when the task is done or when some ex-pected event has taken place.

American National Standards Institute (ANSI) An organization of American industry and business groups dedicated to the develop-ment of trade and communications stan-dards. ANSI is the American representative to the

International Organization for Stan-dardization (ISO). *See also* International Organization for Standardization (ISO).

amplifier A device, such as a repeater or bridge, that amplifies or increases the power of electrical signals, allowing them to travel on additional cable segments at their original strength. Amplifiers strengthen signals that have been weakened by attenuation.

analog Related to a continuously variable physical property, such as voltage, pressure, or rotation. An analog device can represent an infinite number of values within the range the device can handle. *See also* analog line, digital.

analog line A communications line, such as a telephone line, that carries information in analog (continuously variable) form. To minimize distortion and noise interference, an analog line uses amplifiers to strengthen the signal periodically during transmission.

ANSI *See* American National Standards Institute (ANSI).

APPC *See* advanced program-to-program communication (APPC).

AppleShare AppleShare is the Apple net-work operating system. Features include file sharing, client software that is included with every copy of the Apple operating system, and the AppleShare print server, a server-based print spooler.

AppleTalk The Apple network architecture that is included in the Macintosh operating system software. It is a collection of proto-cols that correspond to the OSI model. Thus network capabilities are built into every Macintosh. AppleTalk protocols support LocalTalk, Ethernet (EtherTalk), and Token Ring (TokenTalk).

AppleTalk filing protocol (AFP) Describes how files are stored and accessed on the network. AFP is responsible for the Apple hierarchical filing structure of volumes, folders, and files and provides for file sharing between Macintoshes and MS-DOS– based computers. It provides an interface for communication between AppleTalk and other network operating systems, allowing Macintoshes to be integrated into any network that uses an operating system that recognizes AFP.

application layer The top (seventh) layer of the OSI reference model. This layer serves as the window that application processes use to access network services. It represents the services that directly support user applica-tions, such as software for file transfers, database access, and e-mail.

application programming interface (API) A set of routines that an application program uses to request and carry out lower-level services performed by the operating system.

application protocols Protocols that work at the higher end of the OSI reference model, providing application-to-application interac-tion and data exchange. Popular application protocols include: FTAM (file transfer access and management)— A file access protocol. SMTP (simple mail transfer protocol)—A TCP/IP protocol for transferring e-mail. Telnet—A TCP/IP protocol for logging on to remote hosts and processing data locally. NCP (NetWare core protocol)—The primary protocol used to transmit information between a NetWare server and its clients.

ArcNet (Attached Resource Computer Network) Developed by Datapoint Corporation in 1977, designed as a baseband, token-passing, bus architecture, transmitting at 2.5 Mbps. A successor to the original ArcNet, *ArcNetplus* supports data transmission rates of 20 Mbps. A simple, inexpensive, flexible network architecture designed for workgroup-sized LANs, ArcNet runs on coaxial, twisted-pair, and fiber-optic cable and supports up to 255 nodes. ArcNet technology predates IEEE Project 802 standards but loosely maps to the 802.4 document. *See also* Project 802.

ARP *See* Address Resolution Protocol (ARP).

ARPANET (Advanced Research Projects

Agency Network) Acronym for the Depart-ment of Defense Advanced Research Projects Agency. A pioneering wide area network (WAN), ARPANET was designed to facilitate the exchange of information between universities and other research organizations. ARPANET, which became operational in the 1960s, is the network from which the Internet evolved..

ASCII (American Standard Code for Information Interchange) A coding scheme that assigns numeric values to letters, numbers, punctua-tion marks, and certain other characters. By standardizing the values used for these characters, ASCII enables computers and computer programs to exchange information.

Asymmetric Digital Subscriber Line (ADSL) A recent modem technology that converts existing twisted-pair telephone lines into access paths for multimedia and high-speed data communications. These new connec-tions can transmit more than 8 Mbps to the subscriber and up to 1 Mbps from the subscriber. ADSL is recognized as a physical layer transmission protocol for unshielded twisted-pair media.

asynchronous transfer mode (ATM) An advanced implementation of packet switch-ing that provides high-speed data transmis-sion rates to send fixed-size cells over broadband LANs or WANs. Cells are 53 bytes—48 bytes of data with five additional bytes of address. ATM accommodates voice, data, fax, real-time video, CD-quality audio, imaging, and multimegabit data transmis-sion. ATM uses switches as multiplexers to permit several computers to put data on a network

simultaneously. Most commercial ATM boards transmit data at about 155 Mbps, but theoretically a rate of 1.2 gigabits per second is possible.

asynchronous transmission A form of data transmission in which information is sent one character at a time, with variable time intervals between characters. Asynchronous transmission does not rely on a shared timer that allows the sending and receiving units to separate characters by specific time periods. Therefore, each transmitted character consists of a number of data bits (that compose the character itself), preceded by a start bit and ending in an optional parity bit followed by a 1-, 1.5-, or 2-stop bit.

ATM *See* asynchronous transfer mode (ATM).

attachment unit interface (AUI) The connec-tor used with standard Ethernet that often includes a cable running off the main, or backbone, coaxial cable. Also known as a DIX connector.

attenuation The weakening or degrading (distorting) of a transmitted signal as it travels farther from its point of origin. This could be a digital signal on a cable or the reduction in amplitude of an electrical signal, without the appreciable modification of the waveform. Attenuation is usually measured in decibels. Attenuation of a signal transmit-ted over a long cable is corrected by a repeater, which amplifies and cleans up an incoming signal before sending it farther along the cable.

auditing A process that tracks network activities by user accounts and a routine element of network security. Auditing can produce records of list users who have accessed—or attempted to access— specific resources; help administrators identify unauthorized activity; and track activities such as logon attempts, connection and disconnection from designated resources, changes made to files and directories, server events and modifications, password changes, and logon parameter changes.

AUI *See* attachment unit interface (AUI).

authentication Verification based on user name, passwords, and time and account restrictions.

AWG (American Wire Gauge) A standard that determines wire diameter. The diameter varies inversely to the gauge number..

B

backbone The main cable, also known as the trunk segment, from which transceiver cables connect to computers, repeaters, and bridges.

back end In a client/server application, the part of the program that runs on the server.

backup A duplicate copy of a program, a disk, or data, made to secure valuable files from loss.

backup domain controller (BDC) In a Win-dows NT Server domain, a computer that receives a copy of the domain's security policy and domain database and authenti-cates network logons. It provides a backup if the primary domain controller (PDC) becomes unavailable. A domain is not required to have a BDC, but it is recommended to have a BDC to back up the PDC. *See also* domain, domain controller, primary domain controller.

bandwidth In communications, the difference between the highest and lowest frequencies in a given range. For example, a telephone accommodates a bandwidth of 3000 Hz, or the difference between the lowest (300 Hz) and highest (3300 Hz) frequencies it can carry. In computer networks, greater bandwidth indicates faster or greater data-transfer capability.

barrel connector A component that can connect two pieces of cable to make a longer piece of cable.

baseband A system used to transmit the encoded signals over cable. Baseband uses digital signaling over a single frequency. Signals flow in the form of discrete pulses of electricity or light. With baseband transmission, the entire communication-channel capacity is used to transmit a single data signal.

base I/O port Specifies a channel through which information is transferred between a computer's hardware, such as the network interface card (NIC), and its CPU.

base memory address Defines the address of the location in a computer's memory (RAM) that is used by the NIC. This setting is sometimes called the RAM start address.

basic input/output system (BIOS) On PC-compatible computers, the set of essential software routines that test hardware at startup, start the operating system, and support the transfer of data among hardware devices. The BIOS is stored in read-only memory (ROM) so that it can be executed when the computer is turned on. Although critical to performance, the BIOS is usually invisible to computer users.

baud A measure of data-transmission speed named after the French engineer and telegrapher Jean-Maurice-Emile Baudot. It is a measure of the speed of oscillation of the sound wave on which a bit of data is carried over telephone lines. Because baud was originally used to measure the transmission speed of telegraph equipment, the term sometimes refers to the data-transmission speed of a modem. However, current modems can send at a speed higher than one bit per oscillation,

so baud is being replaced by the more accurate bps (bits per second) as a measure of modem speed.

baud rate Refers to the speed at which a modem can transmit data. Often confused with bps (the number of bits per second transmitted), baud rate actually measures the number of events, or signal changes, that occur in one second. Because one event can actually encode more than one bit in high-speed digital communication, baud rate and bps are not always synonymous, and the latter is the more accurate term to apply to modems. For example, the 9600-baud modem that encodes four-bits per event actually operates at 2400 baud, but transmits at 9600 bps (2400 events times 4 bits per event), and thus should be called a 9600-bps modem.

BBS *See* bulletin board system (BBS).

BDC *See* backup domain controller (BDC).

beaconing The process of signaling computers on a ring system that token passing has been interrupted by a serious error. All computers in an FDDI or Token Ring network are responsible for monitoring the token-passing process. To isolate serious failures in the ring, FDDI and Token Ring use beaconing in which a computer that detects a fault sends a signal, called a beacon, onto the network. The computer continues to send the beacon until it notices a beacon from its upstream neighbor. This process continues until the only computer sending a beacon is the one directly down-stream of the failure. When the beaconing computer finally receives its own beacon, it assumes the problem has been fixed and regenerates a token.

bind To associate two pieces of information with one another.

binding A process that establishes the communication channel between a protocol driver and a NIC driver.

BIOS (basic input/output system) *See* basic input/output system (BIOS).

BISDN *See* broadband Integrated Services Digital Network (BISDN).

bisync (binary synchronous communications protocol) A communications protocol developed by IBM. Bisync transmissions are encoded in either ASCII or EBCDIC. Messages can be of any length and are sent in units called frames, optionally preceded by a message header. Because bisync uses synchronous transmission, in which message elements are separated by a specific time interval, each frame is preceded and followed by special characters that enable the sending and receiving machines to synchronize their clocks.

bit Short for binary digit: either 1 or 0 in the binary number system. In processing and storage, a bit is the smallest unit of information handled by a computer. It is represented physically by an element such as a single pulse sent through a circuit or small spot on a magnetic disk capable of storing either a 1 or 0. Eight bits make a byte.

bits per second (bps) A measure of the speed at which a device can transfer data. *See also* baud rate.

bit time The time it takes for each station to receive and store a bit.

BNC cable connector A connector for coaxial cable that locks when one connector is inserted into another and is rotated 90 degrees.

BNC components A family of components that include the BNC cable connector, BNC T connector, BNC barrel connector, and the BNC terminator. The origin of the acronym "BNC" is unclear; names ascribed to these letters range from "British Naval Connector" to "Bayonet Neill-Councelman."

boot-sector virus A type of virus that resides in the first sector of a floppy disk or hard drive. When the computer is booted, the virus executes. In this common method of transmitting viruses from one floppy disk to another, the virus replicates itself onto the new drive each time a new disk is inserted and accessed..

bottleneck A device or program that significantly degrades network performance. Poor network performance results when a device uses noticeably more CPU time than it should, consumes too much of a resource, or lacks the capacity to handle the load. Potential bottlenecks can be found in the CPU, memory, NIC, and other components.

bounce *See* signal bounce.

bps *See* bits per second (bps).

bridge A device used to join two LANs. It allows stations on either network to access resources on the other. Bridges can be used to increase the length or number of nodes for a network. The bridge makes connections at the data-link layer of the OSI reference model.

bridged network A network that is connected by bridges.

Broadband Integrated Services Digital Network (BISDN) A consultative committee for the CCITT that recommends definitions for voice, data, and video in the megabit/gigabit range. BISDN is also a single ISDN network that can handle voice, data, and video services. BISDN works with an optical cable transport network called Synchronous Optical Network (SONET) and an asynchronous transfer mode (ATM) switching service. SMDS (Switched Multimegabit Data

Services) is a BISDN service that offers high bandwidth to WANs. *See also* Synchronous Optical Network (SONET), asynchronous transfer mode (ATM), Switched Multimegabit Data Services (SMDS).

broadband network A type of LAN on which transmissions travel as analog (radio-frequency) signals over separate inbound and outbound channels. Devices on a broadband network are connected by coaxial or fiber-optic cable, and signals flow across the physical medium in the form of electromagnetic or optical waves. A broadband system uses a large portion of the electromagnetic spectrum with a range of frequencies from 50 Mbps to 600 Mbps. These networks can simultaneously accommodate television, voice, data, and other services over multiple transmission channels.

broadcast A transmission sent simulta-neously to more than one recipient. In communication and on networks, a broadcast message is one distributed to all stations or computers on the network.

broadcast storm An event that occurs when there are so many broadcast messages on the network that they approach or surpass the capacity of the network bandwidth. This can happen when one computer on the network transmits a flood of frames saturating the network with traffic so it can no longer carry messages from any other computer. Such a broadcast storm can shut down a network.

brouter A network component that combines the best qualities of a bridge and a router. A brouter can act as a router for one protocol and as a bridge for all the others. Brouters can route selected routable protocols, bridge nonroutable protocols, and deliver more cost-effective and manageable internetworking than separate bridges and routers. A brouter is a good choice in an environment that mixes several homogeneous LAN segments with two different segments.

buffer A reserved portion of RAM in which data is held temporarily, pending an opportunity to complete its transfer to or from a storage device or another location in memory.

built-in groups One of four kinds of group accounts used by Microsoft Windows NT and Windows NT Server. Built-in groups, as the name implies, are included with the network operating system. Built-in groups have been granted useful collections of rights and built-in abilities. In most cases, a built-in group provides all the capabilities needed by a particular user. For example, if a domain user account belongs to the built-in Administrators group, logging on with that account gives a user administrative capabilities over the domain and the servers in the domain. *See also* user account.

bulletin board system (BBS) A computer system equipped with one or more modems or other means of network access that serves as an information and message-passing center for remote users. Many software and hardware companies run proprietary BBSs for customers that include sales information, technical support, and software upgrades and patches.

bus Parallel wires or cabling that connect components in a computer.

bus topology A topology that connects each computer, or station, to a single cable. At each end of the cable is a terminating resistor, or terminator. A transmission is passed back and forth along the cable, past the stations and between the two terminators, carrying a message from one end of the network to the other. As the message passes each station, the station checks the message's destination address. If the address in the message matches the station's address, the station receives the message. If the addresses do not match, the bus carries the message to the next station, and so on.

byte A unit of information consisting of 8 bits. In computer processing or storage, a byte is equivalent to a single character, such as a letter, numeral, or punctuation mark. Because a byte represents only a small amount of information, amounts of computer memory are usually given in kilobytes (1024 bytes or 2 raised to the 10th power), mega-bytes (1,048,576 bytes or 2 raised to the 20th power), gigabytes (1024 megabytes), terabytes (1024 gigabytes), petabytes (1024 terabytes), or exabytes (1024 petabytes).

C

CA (certificate authority) *See* certificate authority (CA).

cable categories The three major groups of cabling that connect the majority of networks: coaxial, twisted-pair (unshielded twisted-pair and shielded twisted-pair), and fiber-optic cabling.

cable testers *See* advanced cable testers.

cache A special memory subsystem or part of RAM in which frequently used data values are duplicated for quick access. A memory cache stores the contents of frequently accessed RAM locations and the addresses where these data items are stored. When the processor references an address in memory, the cache checks to see whether it holds that address. If it does hold the address, the data is returned to the processor; if it does not, regular memory access occurs. A cache is useful when RAM accesses are slow as compared to the microprocessor speed.

carrier-sense multiple access with collision avoidance (CSMA/CA) access method An access method by which each computer signals its intent to transmit before it actually transmits data, thus avoiding possible transmission collisions. *See also* access method.

carrier-sense multiple access with collision detection (CSMA/CD) access method An access method generally used with bus topologies. Using CSMA/CD, a station "listens" to the physical medium to determine whether another station is currently transmitting a data frame. If no other station is transmitting, the station sends its data. A station "listens" to the medium by testing the medium for the presence of a carrier, a specific level of voltage or light—thus the term carrier-sense. The multiple access indicates that there are multiple stations attempting to access or put data on the cable at the same time. The collision detection indicates that the stations are also listening for collisions. If two stations attempt to transmit at the same time and a collision occurs, the stations must wait a random period of time before attempting to transmit. *See also* access method.

CCEP *See* Commercial COMSEC Endorsement Program (CCEP).

CCITT (Comit› Consultatif Internationale de T›l›graphie et T›l›phonie) An organization based in Geneva, Switzerland, and established as part of the United Nations International Telecommunications Union (ITU). The CCITT recommends use of communication standards that are recognized throughout the world. Protocols established by the CCITT are applied to modems, networks, and facsimile transmission.

Cellular Digital Packet Data (CDPD) A communication standard that uses very fast technology, similar to that of cellular telephones, to offer computer data transmissions over existing analog voice networks between voice calls, when the system is not occupied with voice communication.

central file server A network in which specific computers take on the role of server with other computers on the network sharing the resources. *See also* client/server.

certificate A collection of data used for authentication and secure exchange of information on nonsecured networks, such as the Internet. A certificate securely binds a public key to the entity that holds the corresponding private key. Certificates are digitally signed by the issuing CA and can be managed for a user, computer, or service. The most widely accepted format for certificates is defined by ITUT X.509 international standards.

certificate authority (CA) An entity responsible for establishing the couching for the authenticity of public keys belonging to users or other CAs. Activities of a CA may include binding public keys to distinguished names through signed certificates, managing certificate serial numbers, and revoking certificates.

central processing unit (CPU) The computational and control unit of a computer, the device that interprets and carries out instructions. Single-chip CPUs, called microprocessors, made personal computers possible. Examples include the 80286, 80386, 80486, and Pentium processors.

cladding The concentric layer of glass that surrounds the extremely thin, cylindrical glass core in fiber-optic cable..

client A computer that accesses shared network resources provided by another computer, called a server.

client/server A network architecture designed around the concept of distributed processing in which a task is divided between a back end (server), that stores and distributes data, and a front end (client) that requests specific data from the server. *See also* central file server.

coaxial cable (coax) A conductive center wire surrounded by an insulating layer, a layer of wire mesh (shielding), and a non-conductive outer layer. Coaxial cable is resistant to interference and signal weakening that other cabling, such as unshielded twisted-pair cable, can experience.

codec (compression/decompression) Compression/decompression technology for digital video and stereo audio.

Commercial COMSEC Endorsement Program (CCEP) A data-encryption standard introduced by the National Security Agency. Vendors who have the proper security clearance can join CCEP and be authorized to incorporate classified algorithms into communications systems. *See also* encryption.

companion virus A virus that uses the name of a real program, but has a different file extension from that of the program itself. The virus is activated when its companion program is opened. The companion virus uses a .COM file extension, which overrides the .EXE file extension and activates the virus.

concentrator A network physical-layer device that serves as a central connection for other network devices. *See also* hub.

contention Competition among stations on a network for the opportunity to use a communication line or network resource. Two or more computers attempt to transmit over the same cable at the same time, thus causing a collision on the cable. Such a system needs regulation to eliminate data collisions on the cable

which can destroy data and bring network traffic to a halt. *See also* carrier-sense multiple access with collision detection (CSMA/CD) access method.

core In coaxial cable, the innermost part of the cable that carries the electronic signals which make up the data. It can be solid (usually copper) or stranded. In fiber-optic cable, digital data signals travel through an extremely thin cylindrical glass core surrounded by cladding.

CPU *See* central processing unit (CPU).

CRC *See* cyclical redundancy check (CRC).

crossover cable Used to connect two computers directly with a single patch cable, so that the send wire from one computer is connected to the receive port on the other computer. Crossover cables are useful in troubleshooting network connection problems.

crosstalk Signal overflow from an adjacent wire. When a second faint telephone conversation is heard in the background while one is making a phone call, crosstalk is occurring.

cryptography The processes, art, and science of keeping messages and data secure. Cryptography is used to enable and ensure confidentiality, data integrity, authentication (entity and data origin), and nonrepudiation.

CSMA/CD *See* carrier-sense multiple access with collision detection (CSMA/CD) access method.

cyclical redundancy check (CRC) A form of error checking in transmitting data. The sending packet includes a number produced by a mathematical calculation made at the transmission source. When the packet arrives at its destination, the calculation is redone. If the two figures are the same, this indicates that the data in the packet has remained stable. If the calculation at the destination differs from the calculation at the source, this indicates that the data has changed during the transmission. In that case, the CRC routine signals the source computer to retransmit the data.

D

daisy chain A set of devices, such as Small Computer System Interfaces (SCSIs) and Universal Serial Buses (USBs), that are connected in a series. When devices are daisy-chained to a microcomputer, the first device is connected to the computer, the second device is connected to the first, and so on down the line. Signals are passed through the chain from one device to the next. *See also* Small Computer System Interface (SCSI) and Universal Serial Bus (USB).

database management system (DBMS) A layer of software between the physical database and the user. The DBMS manages all requests for database action from the user, including keeping track of the physical details of file locations and formats, indexing schemes, and so on. In addition, a DBMS permits centralized control of security and data integrity requirements.

Data Communications Equipment (DCE) One of two types of hardware connected by an RS-232 serial connection, the other being a DTE (data terminal equipment) device. A DCE device takes input from a DTE device and often acts as an intermediary device, transforming the input signal in some way before sending it to the actual recipient. For example, an external modem is a DCE device that accepts data from a microcomputer (DTE), modulates it, then sends the data along a telephone connection. In communication, an RS-232 DCE device receives data over line 2 and transmits over line 3. In contrast, a DTE device receives over line 3 and transmits over line 2. *See also* Data Terminal Equipment (DTE).

data encryption *See* encryption.

data encryption standard (DES) A commonly used, highly sophisticated algorithm developed by the U.S. National Bureau of Standards for encrypting and decoding data. *See also* encryption.

data frames Logical, structured packages in which data can be placed. Data being transmitted is segmented into small units and combined with control information such as message start and message end indicators. Each package of information is transmitted as a single unit, called a frame. The data-link layer packages raw bits from the physical layer into data frames. The exact format of the frame used by the network depends on the topology. *See also* frame.

data-link layer The second layer in the OSI reference model. This layer packages raw bits from the physical layer into data frames. *See also* Open Systems Interconnection (OSI) reference model.

data stream An undifferentiated, byte-by-byte flow of data.

Data Terminal Equipment (DTE) According to the RS-232 hardware standard, a device, such as a microcomputer or a terminal, that. has the ability to transmit information in digital form over a cable or a communication line. A DTE is one of two types of hardware connected by an RS-232 serial connection, the other being a DCE (Data Communications Equipment) device, such as a modem, that normally connects the DTE to the communication line itself. In communication, an RS-232 DTE device transmits data over line 2 and receives it over line 3. A DCE receives over line 2 and transmits over line 3. *See also* Data Communications Equipment (DCE).

DB connector A connector that facilitates parallel input and output. The initials DB stand for *data bus*. The numbers which follow DB indicate the number of wires within the connector. For example, a DB-15 connector has 15 pins and supports up to 15 lines, each of which can connect to a pin on the connector; a DB-25 connector has 25 of each.

DBMS *See* database management system (DBMS).

DCE *See* Data Communications Equipment (DCE).

DECnet Digital Equipment Corporation hardware and software products that implement the Digital Network Architecture (DNA). DECnet defines communication networks over Ethernet LANs, Fiber Distributed Data Interface metropolitan area networks (FDDI MANs), and WANs that use private or public data transmission facilities. It can use TCP/IP and OSI protocols as well as Digital's DECnet protocols. *See also* Fiber Distributed Data Interface, metropolitan area network (MAN).

dedicated server A computer on a network that functions only as a server and is not also used as a client. *See also* server, server-based network.

DES *See* data encryption standard (DES).

device A generic term for a computer subsystem. Printers, serial ports, and disk drives are referred to as devices.

Dfs (distributed file system) *See* distributed file system (Dfs).

DHCP *See* Dynamic Host Configuration Protocol (DHCP).

dial-up connection The connection to your network if you are using a device that uses the telephone network. This includes modems with a standard phone line, ISDN cards with high speed ISDN lines, or X.25 networks. If you are a typical user, you may have one or two dial-up connections, perhaps to the Internet and to your corporate network. In a more complex server situation, multiple network modem connections might be used to implement advanced routing.

digital A system that encodes information numerically, such as 0 and 1, in a binary context. Computers use digital encoding to process data. A digital signal is a discrete binary state, either on or off. *See also* analog.

digital line A communication line that carries information only in binary-encoded (digital) form. To minimize distortion and noise interference, a digital line uses repeaters to regenerate the signal periodically during transmission. *See also* analog line.

digital signature A means for originators of a message, file, or other digitally encoded information to bind their identity to the information. The process of signing information entails transforming the information, as well as some secret information held by the sender, into a tag called a signature. Digital signatures are used in public key environments. and they provide nonrepudiation and integrity services.

digital video disc (DVD) An optical storage medium with higher capacity and bandwidth than a compact disc. A DVD can hold a full-length film with up to 133 minutes of high-quality video, in MPEG-2 format, and audio. Also known as digital versatile disc.

digital voltmeter (DVM) A basic, all-purpose electronic measuring tool. In addition to indicating the amount of voltage passing through resistance, in network cable testing, voltmeters measure continuity to determine if a cable is able to carry current.

DIP (dual inline package) switch One or more small rocker or sliding switches that can be set to one of two states—closed or open—to control options on a circuit board.

direct memory access (DMA) Memory access that does not involve the microprocessor, frequently employed for data transfer directly between memory and an "intelligent" peripheral device such as a disk drive.

direct memory access (DMA) channel A channel for direct memory access that does not involve the microprocessor, providing data transfer directly between memory and a disk drive.

disk duplexing *See* disk mirroring, fault tolerance.

disk duplicating *See* disk mirroring.

diskless computers Computers that have neither a floppy disk nor a hard disk. Diskless computers depend on special ROM in order to provide users with an interface through which they can log on to the network.

disk mirroring A technique, also known as disk duplicating, in which all or part of a hard disk is duplicated onto one or more hard disks, each of which ideally is attached to its own controller. With disk mirroring, any change made to the original disk is simultaneously made to the other disk(s). Disk mirroring is used in situations in which a backup copy of current data must be maintained at all times. *See also* disk striping, fault tolerance.

disk striping Divides data into 64 K blocks and spreads it equally in a fixed rate and order among all disks in an array. However, disk striping does not provide any fault tolerance because there is no data redundancy. If any partition in the set fails, all data is lost. *See also* disk mirroring, fault tolerance.

distributed file system (Dfs) A single, logical, hierarchical file system. Dfs organizes shared folders on different computers in a network to provide a logical tree structure for file system resources.

DIX (Digital, Intel, Xerox) connector The connector used with standard Ethernet that often includes a cable running off the main, or backbone, coaxial cable. This is also known as an AUI connector. *See also* attachment unit interface (AUI).

DMA *See* direct memory access (DMA).

DMA channel *See* direct memory access (DMA) channel.

DNS *See* Domain Name System (DNS).

domain For Microsoft networking, a collection of computers and users that share a common database and security policy that are stored on a Windows NT Server domain controller. Each domain has a unique name. *See also* workgroup.

domain controller For Microsoft networking, the Windows NT Server–based computer that authenticates domain logons and main. tains the security policy and master database for a domain. *See also* backup domain controller (BDC), primary domain controller (PDC).

Domain Name System (DNS) A general-purpose distributed, replicated, data-query service used primarily on the Internet for translating host names into Internet addresses.

downtime The amount of time a computer system or associated hardware remains nonfunctioning. Although downtime can occur because hardware fails unexpectedly, it can also be a scheduled event, such as when a network is shut down to allow time for maintaining the system, changing hardware, or archiving files.

driver A software component that permits a computer system to communicate with a device. For example, a printer driver is a device driver that translates computer data into a form understood by the target printer. In most cases, the driver also manipulates the hardware in order to transmit the data to the device.

DTE *See* Data Terminal Equipment (DTE).

dual boot A computer configuration that can start two different operating systems.

dual shielded cable Cable that contains one layer of foil and insulation and one layer of braided metal shielding.

dumb terminal A device used for obtaining or entering data on a network that does not contain any "intelligence" or processing power provided by a CPU.

duplex transmission Also called full-duplex transmission. Communication that takes place simultaneously, in both directions, between the sender and the receiver. Alternative methods of transmission are simplex, which is one-way only, and half-duplex, which is two-way communication that occurs in only one direction at a time.

DVD (digital video disc, also known as digital versatile disc) *See* digital video disc (DVD).

Dynamic Host Configuration Protocol (DHCP) A protocol for automatic TCP/IP configuration that provides static and dynamic address allocation and management. *See also* Transport Control Protocol/Internet Protocol (TCP/IP).

E

EBCDIC *See* Extended Binary Coded Decimal Interchange Code (EBCDIC).

EFS (encrypting file system) *See* encrypting file system (EFS)

EISA *See* Extended Industry Standard Architecture (EISA).

encrypting file system (EFS) Windows 2000 file system that enables users to encrypt files and folders on an NTFS volume disk to keep them safe from access by intruders.

encryption The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or when the data is stored on a transportable magnetic medium. A key is required to decode the information. *See also* CCEP, data encryption standard (DES).

Enhanced Small Device Interface (ESDI) A standard that can be used with high-capacity hard disks and tape drives to enable high-speed communication with a computer. ESDI drivers typically transfer data at about 10 Mbps.

ESDI *See* Enhanced Small Device Interface (ESDI).

Ethernet A LAN developed by Xerox in 1976. Ethernet became a widely implemented network from which the IEEE 802.3 standard for contention networks was developed. It uses a bus topology and the original Ethernet relies on CSMA/CD to regulate traffic on the main communication line.

EtherTalk Allows the AppleTalk network protocols to run on Ethernet coaxial cable. The EtherTalk card allows a Macintosh computer to connect to an 802.3 Ethernet network. *See also* AppleTalk.

event An action or occurrence to which a program might respond. Examples of events are mouse clicks, key presses, and mouse movements. Also, any significant occurrence in the system or in a program that requires users to be notified or an entry to be added to a log.

exabyte *See* byte.

Extended Binary Coded Decimal Interchange Code (EBCDIC) A coding scheme developed by IBM for use with IBM mainframe and Personal Computers as a standard method of assigning binary (numeric) values to alpha-betic, numeric, punctuation, and transmission- control characters.

Extended Industry Standard Architecture (EISA) A 32-bit bus design for x86-based computers introduced in 1988. EISA was specified by an industry consortium of nine computer-industry companies (AST Research, Compaq, Epson, Hewlett-Packard, NEC, Olivetti, Tandy, Wyse, and Zenith). An EISA device uses cards that are upwardly compatible from ISA. *See also* Industry Standard Architecture (ISA).

extended partition A portion of a basic disk that can contain logical drives. Use an extended partition if you want to have more than four volumes on your basic disk. Only one of the four partitions allowed per physical disk can be an extended partition, and no primary partition needs to be present to create an extended partition. Extended partitions can be created only on basic disks.

F

fast Ethernet Also called 100BaseX Ethernet. An extension to the existing Ethernet standard, it runs on UTP Category 5 data-grade cable and uses CSMA/CD in a star-wired bus topology, similar to 10BaseT in which all cables are attached to a hub.

FAT (file allocation table) *See* file allocation table (FAT).

fault tolerance The ability of a computer or an operating system to respond to an event such as a power outage or a hardware failure in such a way that no data is lost and any work in progress is not corrupted.

Fiber Distributed Data Interface (FDDI) A standard developed by the ANSI for high-speed, fiber-optic local area networks. FDDI provides specifications for transmission rates of 100 Mbps on networks based on the Token Ring standard.

fiber-optic cable Cable that uses optical fibers to carry digital data signals in the form of modulated pulses of light.

file allocation table (FAT) A table or list maintained by some operating systems to keep track of the status of various segments of disk space used for file storage.

file infector A type of virus that attaches itself to a file or program and activates any time the file is used. Many subcategories of file infectors exist. *See also* companion virus, macro virus, polymorphic virus, stealth virus.

file replication service (FRS) Provides multi-master file replication for designated directory trees between designated Windows 2000 servers. The designated directory trees must be on disk partitions formatted with the version of NTFS used with Windows 2000. FRS is used by the Microsoft distributed file system (Dfs) to automatically synchronize content between assigned replicas, and by Active Directory services to automatically synchronize content of the system volume information across domain controllers.

File Transfer Protocol (FTP) A process that provides file transfers between local and remote computers. FTP supports several commands that allow bidirectional transfer of binary and ASCII files between computers. The FTP client is installed with the TCP/ IP connectivity utilities. *See also* ASCII (American Standard Code for Information Interchange), Transport Control Protocol/ Internet Protocol (TCP/IP).

firewall A security system, usually a combination of hardware and software, intended to protect a network against external threats coming from another network, including the Internet. Firewalls prevent an organization's networked computers from communicating directly with computers that are external to the network, and vice versa. Instead, all incoming and outgoing communication is routed through a proxy server outside the organization's network. Firewalls also audit network activity, recording the volume of traffic and information about unauthorized attempts to gain access. *See also* proxy server.

firmware Software routines stored in ROM. Unlike RAM, ROM stays intact even in the absence of electrical power. Startup routines and low-level I/O instructions are stored in firmware.

flow control Regulating the flow of data through routers to ensure that no segment becomes overloaded with transmissions.

FQDN (fully qualified domain name) *See* fully qualified domain name (FQDN).

frame A package of information transmitted on a network as a single unit. Frame is a term most often used with Ethernet networks. A frame is similar to the packet used in other networks. *See also* data frame, packet.

frame preamble Header information, added to the beginning of a data frame in the physical layer of the OSI reference model.

frame relay An advanced, fast-packet, variable-length, digital, packet-switching technology. It is a point-to-point system that uses a private virtual circuit (PVC) to transmit variable-length frames at the data-link layer of the OSI reference model. Frame relay networks can also provide subscribers with bandwidth, as needed, that allows users to make nearly any type of transmission.

front end In a client/server application, front end refers to the part of the program carried out on the client computer.

FRS (file replication service) *See* file replication service (FRS).

FTP *See* File Transfer Protocol (FTP).

full-duplex transmission Also called duplex transmission. Communication that takes place simultaneously, in both directions. *See also* duplex transmission.

fully qualified domain name (FQDN) A DNS domain name that has been stated unambiguously so as to indicate with absolute certainty its location in the domain namespace tree. Fully qualified domain names differ from relative names in that they are typically stated with a trailing period (.), for example, host.example.microsoft.com, to qualify their position to the root of the namespace.

G

gateway A device used to connect networks using different protocols so that information can be passed from one system to the other. Gateways functions at the network layer of the OSI reference model.

Gb *See* gigabit.

GB *See* gigabyte.

gigabit 1,073,741,824 bits. Also referred to as 1 billion bits.

gigabyte Commonly, a thousand megabytes. However, the precise meaning often varies with the context. A gigabyte is 1 billion bytes. In the context of computing, bytes are often expressed in multiples of powers of two. Therefore, a gigabyte can also be either 1000 megabytes or 1024 megabytes, where a megabyte is considered to be 1,048,576 bytes (2 raised to the 20th power).

global group One of four kinds of group accounts used by Microsoft Windows NT and Windows NT Server. Used across an entire domain, global groups are created on a Primary Domain Controller (PDC) in the domain in which the user accounts reside. Global groups can contain only user accounts from the domain in which the global group is created. Members of global groups obtain resource permissions when the global group is added to a local group. *See also* group, primary domain controller (PDC).

group In networking, an account containing other accounts that are called members. The permissions and rights granted to a group are also provided to its members; thus, groups offer a convenient way to grant common capabilities to collections of user accounts. For Windows NT, groups are managed with User Manager. For Windows NT Server, groups are managed with User Manager for Domains.

H

half-duplex transmission Two-way communication occurring in only one direction at a time.

handshaking A term applied to modem-to-modem communication. Refers to the process by which information is transmitted between the sending and receiving devices to maintain and coordinate data flow between them. Proper handshaking ensures that the receiving device will be ready to accept data before the sending device transmits.

hard disk One or more inflexible platters coated with material that allows the magnetic recording of computer data. A typical hard disk rotates at up to 7200 revolutions per minute (RPM), and the read/write heads ride over the surface of the disk on a cushion of air 10 to 25 millionths of an inch deep. A hard disk is sealed to prevent contaminants from interfering with the close head-to-disk tolerances. Hard disks provide faster access to data than floppy disks and are capable of storing much more information. Because platters are rigid, they can be stacked so that one hard-disk drive can access more than one platter. Most hard disks have between two and eight platters..

hardware The physical components of a computer system, including any peripheral equipment such as printers, modems, and mouse devices.

hardware compatibility list (HCL) A list of computers and peripherals that have been tested and have passed compatibility testing with the product for which the HCL is being developed. For example, the Windows NT 3.51 HCL lists the products which have been tested and found to be compatible with Window NT 3.51.

hardware loopback A connector on a computer that is useful for troubleshooting hardware problems, allowing data to be transmitted to a line, then returned as received data. If the transmitted data does not return, the hardware loopback detects a hardware malfunction.

HCL *See* hardware compatibility list (HCL).

HDLC *See* High-Level Data Link Control (HDLC).

header In network data transmission, one of the three sections of a packet component. It includes an alert signal to indicate that the packet is being transmitted, the source address, the destination address, and clock information to synchronize transmission.

hermaphroditic connector A connector that is neither male nor female, such as IBM cable connectors in which any two can be connected together, as opposed to BNC connectors that require both a male part and female part before a connection can be made.

hertz (Hz) The unit of frequency measurement. Frequency measures how often a periodic event occurs, such as the manner in which a wave's amplitude changes with time. One hertz equals one cycle per second. Frequency is often measured in kilohertz (KHz, 1000 Hz), megahertz (MHz), giga-hertz (GHz, 1000 MHz), or terahertz (THz, 10,000 GHz).

High-Level Data Link Control (HDLC) HDLC is a widely accepted international protocol, developed by the International Organization for Standardization (ISO), that governs information transfer. HDLC is a bit-oriented, synchronous protocol that applies to the data-link (message packaging) layer of the OSI reference model. Under the HDLC protocol, data is transmitted in frames, each of which can contain a variable amount of data, but which must be organized in a particular way. *See also* data frames, frame. **hop** In routing through a mesh environment, the transmission of a data packet through a router.

host *See* server.

hot fixing *See* sector sparing.

HTML *See* Hypertext Markup Language (HTML).

hub A connectivity component that provides a common connection among computers in a star-configured network. Active hubs require electrical power but are able to regenerate and retransmit network data. Passive hubs simply organize the wiring. *See also* Multistation Access Unit (MAU).

hybrid hub An advanced hub that can accommodate several different types of cables.

hybrid network A network made up of mixed components.

Hypertext Markup Language (HTML) A language developed for writing pages for the World Wide Web. HTML allows text to include codes that define fonts, layout, embedded graphics, and hypertext links. Hypertext provides a method for presenting text, images, sound, and videos that are linked together in a nonsequential web of associations.

Hypertext Transport Protocol (HTTP) The method by which World Wide Web pages are transferred over the network.

I

IAB *See* Internet Architecture Board (IAB).

IBM cabling system Used in a Token Ring environment. Introduced by IBM in 1984 to define cable connectors, face plates, distribution panels, and cable types. Many parameters are similar to non-IBM specifications. Uniquely shaped, the IBM connector is hermaphroditic. *See also* hermaphroditic connector.

ICMP *See* Internet Control Message Protocol (ICMP).

IDE *See* Integrated Device Electronics (IDE).

IEEE *See* Institute of Electrical and Electronics Engineers (IEEE).

IEEE Project 802 A networking model developed by the IEEE. Named for the year and month it began (February 1980), Project 802 defines LAN standards for the physical and data-link layers of the OSI reference model. Project 802 divides the data-link layer into two sublayers: Media Access Control (MAC) and Logical Link Control (LLC).

impedance Impedance has two aspects: the first is resistance, which impedes direct and alternating current. Resistance is always greater than zero. The second is reactance, which impedes alternating current only. Reactance varies with frequency and can be positive or negative.

Industry Standard Architecture (ISA) An unofficial designation for the bus design of the IBM Personal Computer (PC) PC/XT. It allows various adapters to be added to the system by inserting plug-in cards into expansion slots. Commonly, ISA refers to the expansion slots themselves; such slots are called 8-bit slots or 16-bit slots. *See also* Extended Industry Standard Architecture (EISA), Micro Channel Architecture.

infrared transmission Electromagnetic radiation with frequencies in the electromagnetic spectrum in the range just below that of visible red light. In network communications, infrared technology offers extremely high transmission rates and wide bandwidth in line-of-sight communications.

Institute of Electrical and Electronics Engineers (IEEE) An organization of engineering and electronics professionals; noted in networking for developing the IEEE 802.x standards for the physical and data-link layers of the OSI reference model, applied in a variety of network configurations.

Integrated Device Electronics (IDE) A type of disk-drive interface in which the controller electronics reside on the drive itself, eliminating the need for a separate network interface card. The IDE interface is compatible with the Western Digital ST-506 controller.

Integrated Services Digital Network (ISDN) A worldwide digital communication network that evolved from existing telephone services. The goal of the ISDN is to replace current telephone lines, which require digital-to-analog conversions, with completely digital switching and transmission. facilities capable of carrying data ranging from voice to computer transmissions, music, and video. The ISDN is built on two main types of communications channels: B channels, that carry voice, data, or images at a rate of 64 Kbps (kilobits per second), and a D channel, that carries control information, signaling, and link-management data at 16 Kbps. Standard ISDN Basic Rate desktop service is called 2B+D. Computers and other devices connect to ISDN lines through simple, standardized interfaces.

interfaces Boundaries that separate the layers from each other. For example, in the OSI reference model, each layer provides some service or action that prepares the data for delivery over the network to another computer.

intermediate systems Equipment that provides a network communication link, such as bridges, routers, and gateways.

International Organization for Standardization (ISO) An organization made up of standards-setting groups from various countries. For example, the United States member is the American National Standards Institute (ANSI). The ISO works to establish global standards for communications and information exchange. Primary among its accomplishments is development of the widely accepted OSI reference model. Note that the ISO is often wrongly identified as the International Standards Organization, probably because of the abbreviation "ISO"; however, ISO is derived from "isos," which means "equal" in Greek, rather than an acronym.

International Telecommunications Union (ITU) The organization responsible for setting the standards for international telecommunications.

International Telecommunications Union-Telecommunication (ITU-T) The sector of the ITU responsible for telecommunication standards. ITU-T replaces the Comit› Consultatif Internationale de Telegraphie et Telephonie (CCITT). Its responsibilities include standardizing modem design and operations, and standardizing protocols for networks and facsimile transmission. ITU is an international organization within which governments and the private sector coordinate global telecom networks and services.

Internet Architecture Board (IAB) A body that develops and maintains Internet architectural standards as part of the Internet Society (ISOC). It also adjudicates disputes in the standards process.

Internet Control Message Protocol (ICMP) Used by IP and higher-level protocols to send and receive status reports about information being transmitted.

Internet Protocol (IP) The TCP/IP protocol for packet forwarding. *See also* Transport Control Protocol/Internet Protocol (TCP/IP).

Internetworking The intercommunication in a network that is made up of smaller networks.

Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) A protocol stack that is used in Novell networks. IPX is the NetWare protocol for packet forwarding and routing. It is a relatively small and fast protocol on a LAN, is a derivative of Xerox Network System (XNS), and supports routing. SPX is a connection-oriented protocol used to guarantee the delivery of the data being sent. NWLink is the Microsoft implementation of the IPX/SPX protocol.

interoperability The ability of components in one system to work with components in other systems.

interrupt request (IRQ) An electronic signal sent to a computer's CPU to indicate that an event has taken place that requires the processor's attention.

IP *See* Internet Protocol (IP). *See also* Transport Control Protocol/Internet Protocol (TCP/IP).

ipconfig A diagnostic command that displays all current TCP/IP network configuration values. It is of particular use on systems running DHCP because it allows users to determine which TCP/IP configuration values have been configured by the DHCP server. *See also* winipcfg.

IPX/SPX *See* Internetwork Packet Exchange/ Sequenced Packet Exchange (IPX/SPX).

IRQ *See* interrupt request (IRQ).

ISA *See* Industry Standard Architecture (ISA).

ISDN *See* Integrated Services Digital Network (ISDN).

ISO *See* International Organization for Standardization (ISO).

ITU *See* International Telecommunications Union (ITU).

(ITU-T) International Telecommunications Union-Telecommunication *See* International Telecommunications Union-Telecommunication (ITU-T).

J

jitter Instability in a signal wave form over time that can be caused by signal interference or an unbalanced ring in FDDI or Token Ring environments.

jumper A small plastic-and-metal plug or wire for connecting different points in an electronic circuit. Jumpers are used to select a particular circuit or option from several possible configurations. Jumpers can be used on network interface cards to select the type of connection through which the card will transmit, either DIX or BNC.

K

Kevlar A brand name of the DuPont Corporation for the fibers in the reinforcing layer of plastic that surrounds each glass strand of a fiber-optic connector. The name is sometimes used generically.

key In database management, an identifier for a record or group of records in a data file. Most often, the key is defined as the contents of a single field, called the key field in some database management programs and the index field in others. Keys are maintained in tables and are indexed to speed record retrieval. Keys also refer to code that deciphers encrypted data.

kilo (K) Refers to 1000 in the metric system. In computing terminology, because computing is based on powers of 2, kilo is most often used to mean 1024 (2 raised to the 10th power). To distinguish between the two contexts, a lowercase k is often used to indicate 1000, an uppercase K for 1024. A kilobyte is 1024 bytes.

kilobit (Kbit) One thousand twenty-four bits. *See also* bit, kilo.

kilobyte (KB) Refers to 1024 bytes. *See also* byte, kilo.

L

LAN *See* local area network (LAN).

LAN requester *See* requester (LAN requester).

laser transmission Wireless network that uses a laser beam to carry data between devices.

LAT *See* local area transport (LAT).

layering The coordination of various protocols in a specific architecture that allows the protocols to work together to ensure that the data is prepared, transferred, received, and acted upon as intended.

link The communication system that connects two LANs. Equipment that provides the link, including bridges, routers, and gateways.

local area network (LAN) Computers connected in a geographically confined network, such as in the same building, campus, or office park.

local area transport (LAT) A nonroutable protocol from Digital Equipment Corporation.

local group One of four kinds of group accounts used by Microsoft Windows NT and Windows NT Server. Implemented in each local computer's account database, local groups contain user accounts and other global groups that need to have access, rights, and permissions assigned to a resource on a local computer. Local groups cannot contain other local groups.

LocalTalk Cabling components used in an AppleTalk network, including cables, connector modules, and cable extenders. These components are normally used in a bus or tree topology. A LocalTalk segment supports a maximum of 32 devices. Because of LocalTalk's limitations, clients often turn to vendors other than Apple for AppleTalk cabling. Farallon PhoneNet, for example, can accommodate 254 devices.

local user The user at the computer.

Logical Link Control (LLC) sublayer One of two sublayers created by the IEEE 802 project out of the data-link layer of the OSI reference model. The Logical Link Control (LLC) is the upper sublayer that manages data-link communication and defines the use of logical interface points, called service access points (SAPs), used by computers to transfer information from the LLC sublayer to the upper OSI layers. *See also* Media Access Control (MAC) sublayer, service access point (SAP).

lost token Refers to an error on a Token Ring network that causes an errant station to halt the token, leaving the ring without a token.

M

MAC (Message Authentication Code) *See* Message Authentication Code (MAC).

macro virus A file-infector virus named because it is written as a macro for a specific application. Macro viruses are difficult to detect and becoming more common, often infecting widely used applications, such as word-processing programs. When an infected file is opened, the virus attaches itself to the application, then infects any files accessed by that application. *See also* file infector.

magneto-optical (MO) disc A plastic or glass disc, coated with a compound containing special properties, that is read by bouncing a low-intensity laser beam off the disc..

MAN (metropolitan area network) *See* metro-politan area network (MAN).

MAU *See* Multistation Access Unit (MSAU or MAU).

Mb *See* megabit (Mb).

MB *See* megabyte (MB).

Mbps *See* millions of bits per second (Mbps).

media The vast majority of LANs today are connected by some sort of wire or cabling that acts as the LAN transmission medium, carrying data between computers. The cabling is often referred to as the media.

Media Access Control (MAC) driver The device driver located at the Media Access Control sublayer of the OSI reference model. This driver is also known as the NIC driver. It provides low-level access to NICs by providing data-transmission support and some basic NIC management functions. These drivers also pass data from the physical layer to transport protocols at the network and transport layers.

Media Access Control (MAC) sublayer One of two sublayers created by the IEEE 802 project out of the data-link layer of the OSI reference model. The Media Access Control (MAC) sublayer communicates directly with the network interface card and is responsible for delivering error-free data between two computers on the network. *See also* Logical Link Control (LLC) sublayer.

megabit (Mb) Usually, 1,048,576 bits; sometimes interpreted as 1 million bits. *See also* bit.

megabyte (MB) 1,048,576 bytes (2 raised to the 20th power); sometimes interpreted as 1 million bytes. *See also* byte.

mesh network topology Connects remote sites over telecommunication links. Common in wide area networks (WANs), meshes use routers to search among multiple active paths (the mesh) and determine the best path at that particular moment.

Message Authentication Code (MAC) An algorithm that insures the quality of a block of data.

metropolitan area network (MAN) A data network designed for a town or city. In geographic breadth, MANs are larger than local area networks but smaller than wide area networks. MANs are usually characterized by very-high-speed connections using fiber-optic cable or other digital media.

Micro Channel Architecture The design of the bus in IBM PS/2 computers (except Models 25 and 30). The Micro Channel is electrically and physically incompatible with the IBM PC/AT bus. Unlike the PC/AT bus, the Micro Channel functions as either a 16-bit or 32-bit bus. The Micro Channel also can be driven independently by multiple bus master processors. *See also* Extended Industry Standard Architecture (EISA), Industry Standard Architecture (ISA).

Microcom Network Protocol (MNP) The standard for asynchronous data-error control developed by Microcom Systems. The method works so well that other companies have adopted not only the initial version of the protocol, but later versions as well. Currently, several modem vendors incorporate MNP Classes 2, 3, 4, and 5.

Microsoft Management Console (MMC) A framework for hosting administrative tools, called consoles. A console may contain tools, folders or other containers, World Wide Web pages, and other administrative items. These items are displayed in the left pane of the console, called a console tree. A console has one or more windows that can provide views of the console tree. The main MMC window provides commands and tools for authoring consoles. The authoring features of MMC and the console tree itself may be hidden when a console is in User mode.

Microsoft Technical Information Network (TechNet) Provides informational support for all aspects of networking, with an emphasis on Microsoft products.

millions of bits per second (Mbps) The unit of measure of supported transmission rates on the following physical media: coaxial cable, twisted-pair cable, and fiber-optic cable. *See also* bit.

MMC (Microsoft Management Console) *See* Microsoft Management Console (MMC).

MNP *See* Microcom Network Protocol (MNP).

MO (magneto-optical) disc *See* magneto-optical (MO) disc.

mobile computing Incorporates wireless adapters using cellular telephone technology to connect portable computers with the cabled network.

modem A communication device that enables a computer to transmit information over a standard telephone line. Because a computer is digital, it works with discrete electrical signals representing binary 1 and binary 0. A telephone is analog and carries a signal that can have many variations. Modems are needed to convert digital signals to analog and back. When transmitting, modems impose (modulate) a computer's digital signals onto a continuous carrier frequency on the telephone line. When receiving, modems sift out (demodulate) the information from the carrier and transfer it in digital form to the computer.

mounted drive A drive attached to an empty folder on an NTFS volume. Mounted drives function the same as any other drive, but are assigned a label or name instead of a drive letter. The mounted drive's name is resolved to a full file system path instead of just a drive letter. Members of the Administrators group can use Disk Management to create mounted drives or reassign drive letters.

MSAU *See* Multistation Access Unit (MAU).

multiplexer (mux) A device used to divide a transmission facility into two or more channels. It can be a program stored in a computer. Also, a device for connecting a number of communication lines to a computer.

Multistation Access Unit (MAU) The name for a Token Ring wiring concentrator. Also referred to as a hub. MAUs are sometimes referred to as MSAUs.

multitasking A mode of operation offered by an operating system in which a computer works on more than one task at a time. There are two primary types of multitasking: preemptive and nonpreemptive. In preemptive multitasking, the operating system can take control of the processor without the task's cooperation. In nonpreemptive multitasking, the processor is never taken from a task. The task itself decides when to give up the processor. A true multitasking operating system can run as many tasks as it has processors. When there are more tasks than processors, the computer must "time. slice" so that the available processors devote a certain amount of time to one task and then move on to the next task, alternating between tasks until all the tasks are completed.

mux *See* multiplexer (mux).

N

Name Binding Protocol (NBP) An Apple protocol responsible for keeping track of entities on the network and matching names with Internet addresses. It works at the transport layer of the OSI reference model.

namespace A set of unique names for resources or items used in a shared computing environment. For MMC, the namespace is represented by the console tree, which displays all of the snap-ins and resources that are accessible to a console. *See also* console tree; MMC; resource; snap-in. For DNS, namespace is the vertical or hierarchical structure of the domain name tree. For example, each domain label, such as host1 or example, used in a fully qualified domain name, such as host1.example.microsoft.com, indicates a branch in the domain namespace tree.

narrowband (single-frequency) transmission High-frequency radio transmission similar to broadcasting. The user tunes both the transmitter and the receiver to a certain frequency to send and receive data.

NAS (network access server) *See* network access server (NAS).

NBP *See* Name Binding Protocol (NBP).

nbtstat A diagnostic command that displays protocol statistics and current TCP/IP connections using NBT (NetBIOS over TCP/IP). This command is available only if the TCP/IP protocol has been installed. *See also* netstat.

NDIS *See* Network Device Interface Specification (NDIS).

NetBEUI (NetBIOS extended user interface) A protocol supplied with all Microsoft network products. NetBEUI advantages include small stack size (important for MS-DOS–based computers), speed of data transfer on the network medium, and compatibility with all Microsoft-based networks. The major drawback of NetBEUI is that it is a LAN transport protocol and therefore does not support routing. It is also limited to Microsoft-based networks.

NetBIOS (network basic input/output system) An application programming interface (API) that can be used by application programs on a LAN consisting of IBM-compatible micro-computers running MS-DOS, OS/2, or some version of UNIX. Primarily of interest to programmers, NetBIOS provides application programs with a uniform set of commands for requesting the lower-level network services required to conduct sessions between nodes on a network and transmit information between them.

netstat A diagnostic command that displays protocol statistics and current TCP/IP network connections. This command is available only if the TCP/IP protocol has been installed. *See also* nbtstat.

NetWare Core Protocol (NCP) Defines the connection control and service-request encoding that make it possible for clients and servers to interact. This is the protocol that provides transport and session services. NetWare security is also provided within this protocol.

network In the context of computers, a system in which a number of independent computers are linked together to share data and peripherals, such as hard disks and printers.

network access server (NAS) The device that accepts PPP connections and places clients on the network that the NAS serves.

network adapter card *See* network interface card (NIC).

network analyzers Network troubleshooting tools, sometimes called protocol analyzers. They perform a number of functions in real-time network traffic analysis and carry out packet capture, decoding, and transmission. They can also generate statistics based on the network traffic to help create a picture of the network's cabling, software, file server, clients, and NICs. Most analyzers have a built-in TDR. *See also* time-domain reflectometer (TDR).

Network Device Interface Specification (NDIS) A standard that defines an interface for communication between the Media Access Control (MAC) sublayer and protocol drivers. NDIS allows for a flexible environment of data exchange. It defines the software interface, called the NDIS interface, which is used by protocol drivers to communicate with the network interface card. The advantage of NDIS is that it offers protocol multiplexing so that multiple protocol stacks can be used at the same time. *See also* Open Data-Link Interface (ODI).

network interface card (NIC) An expansion card installed in each computer and server on the network. The NIC acts as the physical interface or connection between the computer and the network cable.

network layer The third layer in the OSI reference model. This layer is responsible for addressing messages and translating logical addresses and names into physical addresses. This layer also determines the route from the source to the destination computer. It determines which path the data should take based on network conditions, priority of service, and other factors. It also manages traffic problems such as switching, routing, and controlling the congestion of data packets on the network. *See also* Open Systems Interconnection (OSI) reference model.

network monitors Monitors that track all or a selected part of network traffic. They examine frame-level packets and gather information about packet types, errors, and packet traffic to and from each computer.

Network News Transfer Protocol (NNTP) A protocol defined in RFC 977. It is a de facto protocol standard on the Internet used for the distribution, inquiry, retrieval, and posting of Usenet news articles over the Internet.

NIC *See* network interface card (NIC).

NNTP *See* Network News Transfer Protocol (NNTP).

node On a LAN, a device that is connected to the network and is capable of communicating with other network devices. For example, clients, servers, and repeaters are called nodes.

noise Random electrical signals that can get onto the cable and degrade or distort the data. Noise is generated by power lines, elevators, air conditioners, or any device with an electric motor, relays, and radio transmitters. *See also* shielding.

nonpreemptive multitasking A form of multitasking in which the processor is never taken from a task. The task itself decides when to give up the processor. Programs written for nonpreemptive multitasking. systems must include provisions for yielding control of the processor. No other program can run until the non-preemptive program gives up control of the processor. *See also* multitasking, preemptive multitasking.

Novell NetWare One of the leading network architectures.

O

ODI *See* Open Data-Link Interface (ODI).

ohm The unit of measure for electrical resistance. A resistance of 1 ohm will pass 1 ampere of current when a voltage of 1 volt is applied. A 100-watt incandescent bulb has a resistance of approximately 130 ohms.

Open Data-Link Interface (ODI) A specification defined by Novell and Apple to simplify driver development and to provide support for multiple protocols on a single network interface card. Similar to NDIS in many respects, ODI allows Novell NetWare drivers to be written without concern for the protocol that will be used on top of them.

Open Shortest Path First (OSPF) A routing protocol for IP networks, such as the Internet, that allows a router to calculate the shortest path to each node for sending messages.

Open Systems Interconnection (OSI) reference model A seven-layer architecture that standardizes levels of service and types of interaction for computers exchanging information through a network. It is used to describe the flow of data between the physical connection to the network and the end-user application. This model is the best known and most widely used model for describing networking environments.

OSI layer Focus 7. application layer Program-to-program transfer of information 6. presentation layer Text formatting and display code conversion 5. session layer Establishing, maintaining, and coordinating communication 4. transport layer Accurate delivery, service quality 3. network layer Transport routes, message handling, and transfer 2. data-link layer Coding, addressing, and transmitting information 1. physical layer Hardware connections.

optical drive A drive that accommodates optical discs.

optical fiber Medium that carries digital data signals in the form of modulated pulses of light. An optical fiber consists of an extremely thin cylinder of glass, called the core, surrounded by a concentric layer of glass, known as the cladding.

oscilloscope An electronic instrument that measures the amount of signal voltage per unit of time and displays the results on a monitor.

OSI *See* Open Systems Interconnection (OSI) reference model.

OSPF *See* Open Shortest Path First (OSPF).

P

packet A unit of information transmitted as a whole from one device to another on a network. In packet-switching networks, a packet is defined more specifically as a transmission unit of fixed maximum size that consists of binary digits representing data; a header containing an identification number, source, and destination addresses; and sometimes error-control data. *See also* frame.

packet assembler/disassembler (PAD) A device that breaks large chunks of data into packets, usually for transmission over an X.25 network, and reassembles them at the other end. *See also* packet switching.

Packet Internet Groper (ping) A simple utility that tests if a network connection is complete, from the server to the workstation, by sending a message to the remote computer. If the remote computer receives the message, it responds with a reply message. The reply consists of the remote workstation's IP address, the number of bytes in the message, how long it took to reply—given in milliseconds (ms)—and the length of time-to-live (TTL) in seconds. Ping works at the IP level and will often respond even when higher level TCP-based services cannot.

packet switching A message delivery technique in which small units of information (packets) are relayed through stations in a computer network along the best route available between the source and the destination. Data is broken into smaller units and then repacked in a process called packet assembly and disassembly (PAD). Although each packet can travel along a different path, and the packets composing a message can arrive at different times or out of sequence, the receiving computer reassembles the original message. Packet-switching networks are considered fast and efficient. Standards for packet switching on networks are documented in the CCITT recommendation X.25.

PAD *See* packet assembler/disassembler (PAD).

page-description language (PDL) A language that communicates to a printer how printed output should appear. The printer uses the PDL to construct text and graphics to create the page image. PDLs are like blueprints in that they set parameters and features such as type sizes and fonts, but leave the drawing to the printer.

parity An error-checking procedure in which the number of 1s must always be the same— either odd or even—for each group of bits transmitted without error. Parity is used for checking data transferred within a computer or between computers.

partition A portion of a physical disk that functions as if it were a physically separate unit.

partition boot sector A portion of a hard disk partition that contains information about the disk's file system and a short machine language program that loads the Windows operating system.

password-protected share Access to a shared resource that is granted when a user enters the appropriate password.

PBX Private Branch Exchange (PABX Private Automated Branch Exchange) A switching telephone network that allows callers within an organization to place intraorganizational calls without going through the public telephone system.

PDA *See* Personal Digital Assistant (PDA).

PDC *See* Primary Domain Controller (PDC).

PDL *See* page-description language (PDL).

PDN *See* public data network (PDN).

peer-to-peer network A network in which there are no dedicated servers or hierarchy among the computers. All computers are equal and, therefore, known as peers. Generally, each computer functions as both client and server.

Per-Seat Licensing A licensing mode that requires a separate Client Access License for each client computer that accesses Windows 2000 Server, regardless of whether all the clients access the server at the same time.

Per-Server Licensing A licensing mode that requires a separate Client Access License for each concurrent connection to the server, regardless of whether there are other client computers on the network that do not happen to connect concurrently.

performance monitor A tool for monitoring network performance that can display statistics, such as the number of packets sent and received, server-processor utilization, and the amount of data going into and out of the server.

peripheral A term used for devices such as disk drives, printers, modems, mouse devices, and joysticks that are connected to a computer and controlled by its microprocessor.

Peripheral Component Interconnect (PCI) 32-bit local bus used in most Pentium computers and in the Apple Power Macintosh. Meets most of the requirements for providing Plug and Play functionality.

permanent virtual circuit (PVC) A permanent logical connection between two nodes on a packet-switching network; similar to leased lines that are permanent and virtual, except that with PVC the customer pays only for the time the line is used. This type of connection service is gaining importance because both frame relay and ATM use it. *See also* packet switching, virtual circuit.

permissions *See* access permissions.

Personal Digital Assistant (PDA) A type of hand-held computer that provides functions including personal organization features— like a calendar, note taking, database manipulation, calculator, and communications. For communication, a PDA uses cellular or wireless technology that is often built into the system, but that can be supplemented or enhanced by means of a PC Card.

petabyte *See* byte.

phase change rewritable (PCR) A type of rewritable optical technology in which the optical devices come from one manufacturer (Matsushita/Panasonic) and the media comes from two (Panasonic and Plasmon).

physical layer The first (bottommost) layer of the OSI reference model. This layer addresses the transmission of the unstructured raw bit stream over a physical medium (the networking cable). The physical layer relates the electrical/optical, mechanical, and functional interfaces to the cable and also carries the signals that transmit data generated by all of the higher OSI layers. *See also* Open Systems Interconnection (OSI) reference model.

piercing tap A connector for coaxial cable that pierces through the insulating layer and makes direct contact with the conducting core.

ping *See* Packet Internet Groper (ping).

PKI (public key infrastructure) *See* public key infrastructure (PKI).

plenum The space in many buildings between the false ceiling and the floor above, used to circulate warm and cold air throughout the building. The space is often used for cable runs. Local fire codes specify the types of wiring that can be routed through this area.

Plug and Play (PnP) Refers to the ability of a computer system to automatically configure a device added to it. Plug and Play capability exists in Macintoshes based on the NuBus and, since Windows 95, on PC-compatible computers. Also, refers to specifications developed by Intel and Microsoft that allow a PC to configure itself automatically to work with peripherals such as monitors, modems, and printers.

point-to-point configuration Dedicated circuits that are also known as private, or leased, lines. They are the most popular WAN communication circuits in use today. The carrier guarantees full-duplex bandwidth by setting up a permanent link from each end point, using bridges and routers to connect LANs through the circuits. *See also* Point-to-Point Protocol (PPP), Point-to-Point Tunneling Protocol (PPTP), and duplex transmission.

Point-to-Point Protocol (PPP) A data-link protocol for transmitting TCP/IP packets over dial-up telephone connections, such as between a computer and the Internet. PPP was developed by the Internet Engineering Task Force in 1991.

Point-to-Point Tunneling Protocol (PPTP) PPTP is an extension of the Point-to-Point Protocol that is used for communications on the Internet. It was developed by Microsoft to support virtual private networks (VPNs), which allow individuals and organizations to use the Internet as a secure means of communication. PPTP supports encapsulation of encrypted packets in secure wrappers that can be transmitted over a TCP/IP connection. *See also* Virtual Private Networks (VPN).

polymorphic virus A variant of file-infector virus that is named for the fact that it changes its appearance each time it is replicated. This makes it difficult to detect, because no two versions of the virus are exactly the same. *See also* file infector.

preemptive multitasking A form of multitasking (the ability of a computer's operating system to work on more than one task at a time). With preemptive multitasking—as opposed to nonpreemptive multitasking—the operating system can take control of the processor without the task's cooperation. *See also* nonpreemptive multitasking.

presentation layer The sixth layer of the OSI reference model. This layer determines the form used to exchange data between networked computers. At the sending computer, this layer translates data from a format sent down from the application layer into a commonly recognized, intermediary format. At the receiving end, this layer translates the intermediary format into a format useful to that computer's application layer. The presentation layer manages network security issues by providing services such as data encryption, provides rules for data transfer, and performs data compression to reduce the number of bits that need to be transmitted. *See also* Open Systems Interconnection (OSI) reference model.

primary domain controller (PDC) The server that maintains the master copy of the domain's user-accounts database and that validates logon requests. Every network domain is required to have one, and only one, PDC. *See also* domain, domain controller.

primary partition A volume you create using unallocated space on a basic disk. Windows 2000 and other operating systems can start from a primary partition. You can create up to four primary partitions on a basic disk, or three primary partitions and an extended partition. Primary partitions can be created. only on basic disks and cannot be subpartitioned.

print queue A buffer in which a print job is held until the printer is ready to print it.

private key The secret half of a cryptographic key pair that is used with a public key algorithm. Private keys are typically used to decrypt a symmetric session key, digitally sign data, or decrypt data that has been encrypted with the corresponding public key.

Project 802 A subgroup of the IEEE, originally formed in 1980, that defined network standards for the physical components of a network, the network interface card, and the cabling, which are accounted for in the physical and data-link layers of the OSI reference model.

protocol The system of rules and procedures that govern communication between two or more devices. Many varieties of protocols exist, and not all are compatible, but as long as two devices are using the same protocol, they can exchange data. Protocols exist within protocols as well, governing different aspects of communication. Some protocols, such as the RS-232 standard, affect hardware connections. Other standards govern data transmission, including the parameters and handshaking signals such as XON/OFF used in asynchronous (typically, modem) communications, as well as such data-coding methods as bit- and byte-oriented protocols. Still other protocols, such as the widely used XMODEM, govern file transfer, and others, such as CSMA/CD, define the methods by which messages are passed around the stations on a LAN. Protocols represent attempts to ease the complex process of enabling computers of different makes and models to communicate. Additional examples of protocols include the OSI model, IBM's SNA, and the Internet suite, including TCP/IP. *See also* Systems Network Architecture (SNA), Transport Control Protocol/ Internet Protocol (TCP/IP).

protocol analyzers *See* network analyzers.

protocol driver The driver responsible for offering four or five basic services to other layers in the network, while "hiding" the details of how the services are actually implemented. Services performed include session management, datagram service, data segmentation and sequencing, acknowledgment, and possibly routing across a WAN.

protocol stack A layered set of protocols that work together to provide a set of network functions.

proxy server A firewall component that manages Internet traffic to and from a local area network (LAN). The proxy server decides whether it is safe to let a particular message or file pass through to the organization's network, providing access control to the network, and filters and discards requests as specified by the owner, including requests for unauthorized access to proprietary data. *See also* firewall.

public data network (PDN) A commercial packet-switching or circuit-switching WAN service provided by local and long-distance telephone carriers.

public key The nonsecret half of a cryptographic key pair that is used with a public key algorithm. Public keys are typically used when encrypting a session key, verifying a digital signature, or encrypting data that can be decrypted with the corresponding private key.

public key cryptography A method of cryptography in which two different keys are used: a public key for encrypting data and a private key for decrypting data.

public key infrastructure (PKI) The term generally used to describe the laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. In practice, it is a system of digital certificates, certification authorities, and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction. Standards for PKI are still evolving, even though they are being widely implemented as a necessary element of electronic commerce. Public key infrastructure is also called PKI.

punchdown block A wiring terminal, or series of terminals, into which cable can be plugged or "punched down." It is designed for environments that require a centralized location for all cabling to facilitate making changes; wiring running to the jacks can be more easily organized and maintained.

punchdown tool A specialized tool used to "punch down" cable wires into a wiring terminal. Using this tool ensures a solid connection.

PVC (permanent virtual circuit) *See* permanent virtual circuit (PVC).

PVC (polyvinyl chloride) The material most commonly used for insulating and jacketing cable.

Q

QoS (Quality of Service) *See* Quality of Service (QoS).

quad shielding Cable that contains two layers of foil insulation and two layers of braided metal shielding.

Quality of Service (QoS) A set of quality-assurance standards and mechanisms for data transmission, implemented in Windows 2000.

R

RADIUS (Remote Authentication Dial-In User Service) *See* Remote Authentication Dial-In User Service (RADIUS).

RAID *See* redundant array of independent disks (RAID).

random access memory (RAM) Semiconductor- based memory that can be read and written to by the microprocessor or other hardware devices. The storage locations can be accessed in any order. Note that the various types of ROM memory are also capable of random access. However, the term RAM is generally understood to refer to volatile memory, which can be written as well as read. *See also* read-only memory (ROM).

read-only memory (ROM) Semiconductor-based memory that contains instructions or data which can be read but not modified. *See also* random access memory (RAM).

redirector Networking software that accepts I/O requests for remote files, named pipes, or mail slots and sends (redirects) the requests to a network service on another computer.

Reduced Instruction Set Computing (RISC) A type of microprocessor design that focuses on rapid and efficient processing of a relatively small set of instructions. RISC design is based on the premise that most of the instructions that a computer decodes and executes are simple. As a result, RISC. architecture limits the number of instructions that are built into the microprocessor, but optimizes each so it can be carried out very rapidly, usually within a single clock cycle. RISC chips execute simple instructions faster than microprocessors designed to handle a much wider array of instructions. They are, however, slower than general-purpose CISC (complex instruction set computing) chips when executing complex instructions, which must be broken down into many machine instructions before they can be carried out by RISC microprocessors.

redundancy system A fault-tolerant system that protects data by duplicating it in different physical sources. Data redundancy allows access to data even if part of the data system fails. *See also* fault tolerance.

redundant array of independent disks (RAID) A standardization of fault-tolerant options in five levels. The levels offer various combinations of performance, reliability, and cost. Formerly known as redundant array of inexpensive disks (RAID).

redundant array of inexpensive disks (RAID) *See* redundant array of independent disks (RAID).

Remote Authentication Dial-In User Service (RADIUS) A security authentication protocol based on clients and servers and widely used by Internet service providers (ISPs) on non-Microsoft remote servers. RADIUS is the most popular means of authenticating and authorizing dial-up and tunneled network users today.

remote-boot PROM (programmable read-only memory) A special chip in the network interface card that contains the hardwired code that starts the computer and connects the user to the network, used in computers for which there are no hard-disk or floppy drives. *See also* diskless computers.

remote user A user who dials in to the server over modems and telephone lines from a remote location.

repeater A device that regenerates signals so that they can be transmitted on additional cable segments to extend the cable length or to accommodate additional computers on the segment. Repeaters operate at the physical layer of the OSI reference model and connect like networks, such as an Ethernet LAN to an Ethernet LAN. Repeaters do not translate or filter data. For a repeater to work, both segments that the repeater joins must have the same media-access scheme, protocol, and transmission technique.

requester (LAN requester) Software that resides in a computer and forwards requests for network services from the computer's application programs to the appropriate server. *See also* redirector.

resources Any part of a computer system. Users on a network can share computer resources, such as hard disks, printers, modems, CD-ROM drives, and even the processor.

rewritable optical disc An optical disc that can be written to more than once.

RG-58 A/U Stranded-core coaxial cable. The version of this cable used by the United States military is known as RG-58 C/U.

RG-58 /U Solid-core coaxial cable.

rights Authorization with which a user is entitled to perform certain actions on a computer network. Rights apply to the system as a whole, whereas permissions apply to specific objects. For example, a user. might have the right to back up an entire computer system, including the files that the user does not have permission to access. *See also* access permissions.

ring topology A topology in which computers are placed on a circle of cable. There are no terminated ends. The data travels around the loop in one direction and passes through each computer. Each computer acts as a repeater to boost the signal and send it on. Because the signal passes through each computer, the failure of one computer can bring the entire network down. The ring can incorporate features that disconnect failed computers so that the network can continue to function despite the failure. *See also* token passing, Token Ring network.

RIP *See* Routing Information Protocol (RIP).

RISC *See* Reduced Instruction Set Computing (RISC).

RJ-11 A four-wire modular connector used to join a telephone line to a wall plate or a communications peripheral such as a modem.

RJ-45 An eight-wire modular connector used to join a telephone line to a wall plate or some other device. It is similar to an RJ-11 telephone connector but has twice the number of conductors.

ROM *See* read-only memory (ROM).

routable protocols The protocols that support multipath LAN-to-LAN communications. *See also* protocol.

router A device used to connect networks of different types, such as those using different architectures and protocols. Routers work at the network layer of the OSI reference model. This means they can switch and route packets across multiple networks, which they do by exchanging protocol-specific information between separate networks. Routers determine the best path for sending data and filter broadcast traffic to the local segment.

Routing Information Protocol (RIP) A protocol that uses distance-vector algorithms to determine routes. With RIP, routers transfer information among other routers to update their internal routing tables and use that information to determine the best routes based on hop counts between routers. TCP/ IP and IPX support RIP.

RS-232 standard An industry standard for serial communication connections. Adopted by the Electrical Industries Association (EIA), this recommended standard defines the specific lines and signal characteristics used by serial communications controllers to standardize the transmission of serial data between devices.

S

safe mode A method of starting Windows 2000 using basic files and drivers only, without networking. Safe mode is available by pressing the F8 key when prompted during startup. This allows you to start your computer when a problem prevents it from starting normally.

SAP (service access point) *See* service access point (SAP).

SAP (Service Advertising Protocol) *See* Service Advertising Protocol (SAP).

SCSI *See* Small Computer System Interface (SCSI).

SDLC *See* Synchronous Data Link Control (SDLC)..

sector A portion of the data-storage area on a disk. A disk is divided into sides (top and bottom), tracks (rings on each surface), and sectors (sections of each ring). Sectors are the smallest physical storage units on a disk and are of fixed size—typically capable of holding 512 bytes of information apiece.

sector sparing A fault-tolerant system also called hot fixing. It automatically adds sector-recovery capabilities to the file system during operation. If bad sectors are found during disk I/O, the fault-tolerant driver will attempt to move the data to a good sector and map out the bad sector. If the mapping is successful, the file system is not alerted. It is possible for SCSI devices to perform sector sparing, but AT devices (ESDI and IDE) cannot.

security Making computers and data stored on them safe from harm or unauthorized access.

security identifier *or* **security ID (SID)** A unique number that identifies user, group, and computer accounts. Every account on your network is issued a unique SID when the account is first created. Internal processes in Windows 2000 refer to an account's SID rather than the account's user or group name. If you create an account, delete it, and then create an account with the same user name, the new account will not have the rights or permissions previously granted to the old account because the accounts have different SID numbers.

segment The length of cable on a network between two terminators. A segment can also refer to messages that have been broken up into smaller units by the protocol driver.

Sequenced Packet Exchange (SPX) Part of Novell's IPX/SPX protocol suite for sequenced data. *See also* Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX).

Serial Line Internet Protocol (SLIP) Defined in RFC 1055. SLIP is normally used on Ethernet, over a serial line; for example, an RS-232 serial port connected to a modem.

serial transmission One-way data transfer. The data travels on a network cable with one bit following another.

server A computer that provides shared resources to network users. *See also* client.

server-based network A network in which resource security and most other network functions are provided by dedicated servers. Server-based networks have become the standard model for networks serving more than 10 users. *See also* peer-to-peer network.

server message block (SMB) The protocol developed by Microsoft, Intel, and IBM that defines a series of commands used to pass information between network computers. The redirector packages SMB requests into a network control block (NCB) structure that can be sent over the network to a remote device. The network

provider listens for SMB messages destined for it and removes the data portion of the SMB request so that it can be processed by a local device.

service access point (SAP) The interface between each of the seven layers in the OSI protocol stack that has connection points, similar to addresses, used for communication between layers. Any protocol layer can have multiple SAPs active at one time.

Service Advertising Protocol (SAP) Allows service-providing nodes (including file, printer, gateway, and application servers) to advertise their services and addresses.

session A connection or link between stations on the network.

session layer The fifth layer of the OSI reference model. This layer allows two applications on different computers to establish, use, and end a connection called a session. This layer performs name recognition and functions, such as security, needed to allow two applications to communicate over the network. The session layer provides synchronization between user tasks. This layer also implements dialog control between communicating processes, regulating which side transmits, when, for how long, and so on. *See also* Open Systems Interconnection (OSI) reference model.

session management Establishing, maintaining, and terminating connections between stations on the network.

share To make resources, such as folders and printers, available to others.

sharing Means by which files are publicly posted on a network for access by anyone on the network.

shell A piece of software, usually a separate program, that provides direct communication between the user and the operating system. This usually, but not always, takes the form of a command-line interface. Examples of shells are Macintosh Finder and the MS-DOS command interface program COMMAND.COM.

shielded twisted-pair (STP) cable An insulated cable with wires that are twisted around each other with a minimum number of twists per foot. The twists reduce signal interference between the wires, and the more twists per foot, the greater the reduction in interference (crosstalk).

shielding The woven or stranded metal mesh that surrounds some types of cabling. Shielding protects transmitted data by absorbing stray electronic signals, sometimes called noise (random electrical signals that can degrade or distort communications), so that they do not get onto the cable and distort the data.

short A disruption in an electrical circuit that occurs when any two conducting wires or a conducting wire and ground come in contact with each other.

SID (security identifier *or* **security ID)** *See* security identifier *or* security ID (SID).

signal bounce The process by which, on a bus network, the signal is broadcast to the entire network. The signal travels from one end of the cable to the other. If the signal were allowed to continue uninterrupted, it would keep bouncing back and forth along the cable and prevent other computers from sending signals. To stop the signal from bouncing, a component called a terminator is placed at each end of the cable to absorb free signals. Absorbing the signal clears the cable so that other computers can send data. *See also* terminator.

Simple Mail Transfer Protocol (SMTP) A TCP/ IP protocol for transferring e-mail. *See also* application protocols, Transport Control Protocol/Internet Protocol (TCP/IP).

Simple Network Management Protocol (SNMP) A TCP/IP protocol for monitoring networks. SNMP uses a request and response process. In SNMP, short utility programs, called agents, monitor the network traffic and behavior in key network components in order to gather statistical data which they put into a management information base (MIB). To collect the information into a usable. form, a special management console program regularly polls the agents and downloads the information in their MIBs. If any of the data falls either above or below parameters set by the manager, the management console program can present signals on the monitor locating the trouble and notify designated support staff by automatically dialing a pager number.

simplex transmission One-way transmission of data.

simultaneous peripheral operation on line (spool) Facilitates the process of moving a print job from the network into a printer.

SLIP *See* Serial Line Internet Protocol (SLIP).

Small Computer System Interface (SCSI) A standard, high-speed parallel interface defined by the ANSI. A SCSI interface is used for connecting microcomputers to peripheral devices, such as hard disks and printers, and to other computers and LANs. SCSI is pronounced "scuzzy."

smart card A credit card-sized device used to securely store public and private keys, passwords, and other types of personal information. To use a smart card, you need a smart card reader attached to the computer and a personal PIN number for the smart card. In Windows 2000, smart cards can be used to enable certificate-based authentication and single sign-on to the enterprise.

smart card reader A standard device within the smart card subsystem. A smart card reader is an interface device (IFD) that supports bidirectional input/output to a smart card.

SMB *See* server message block (SMB).

SMDS *See* Switched Multimegabit Data Services (SMDS).

SMP *See* symmetric multiprocessing (SMP).

SMTP *See* Simple Mail Transfer Protocol (SMTP).

SNA *See* Systems Network Architecture (SNA).

SNMP *See* Simple Network Management Protocol (SNMP).

software Computer programs or sets of instructions that allow the hardware to work. Software can be grouped into four categories: system software, such as operating systems, that control the workings of the computer; application software, such as word-processing programs, spreadsheets, and databases, which perform the tasks for which people use computers; network software, which enables groups of computers to communicate; and language software, which provides programmers with the tools they need to write programs.

SONET *See* Synchronous Optical Network (SONET).

spanning tree algorithm (STA) An algorithm (mathematical procedure) implemented to eliminate redundant routes and avoid situations in which multiple LANs are joined by more than one path by the IEEE 802.1 Network Management Committee. Under STA, bridges exchange certain control information in an attempt to find redundant routes. The bridges determine which would be the most efficient route, then use that one and disable the others. Any of the disabled routes can be reactivated if the primary route becomes unavailable.

spread-spectrum radio technology A tech-nology that provides for a truly wireless network. Spread-spectrum radio broadcasts. signals over a range of frequencies, avoiding the communication problems of narrowband radio transmission.

SPX *See* Sequenced Packet Exchange (SPX).

SQL *See* structured query language (SQL).

STA *See* spanning tree algorithm (STA).

stand-alone computer A computer that is not connected to any other computers and is not part of a network.

stand-alone environment A work environment in which each user has a personal computer but works independently, unable to share files and other important information that would be readily available through server access in a networking environment.

standard Ethernet A network topology that transmits at 10 Mbps over a baseband wire and can carry a signal 500 meters (five 100- meter segment*s). See also* thicknet.

star topology A topology in which each computer is connected by cable segments to a centralized component called a hub. Signals transmitted by a computer on the star pass through the hub to all computers on the network. This topology originated in the early days of computing with terminals connected to a centralized mainframe. The star topology offers centralized resources and management. However, because each computer is connected to a central point, much cable is required in a large installation, and if the central point fails, the entire network goes down. *See also* hub.

stealth virus A variant of file-infector virus. This virus is so named because it attempts to hide from detection. When an antivirus program attempts to find it, the stealth virus tries to intercept the probe and return false information indicating that it does not exist.

STP *See* shielded twisted-pair (STP).

stripe set A form of fault tolerance that combines multiple areas of unformatted free space into one large logical drive, distributing data storage across all drives simultaneously. In Windows NT, a stripe set requires at least two physical drives and can use up to 32 physical drives. Stripe sets can combine areas on different types of drives, such as Small Computer System Interface (SCSI), Enhanced Small Device Interface (ESDI), and Integrated Device Electronics (IDE) drives.

structured query language (SQL) A database sublanguage used to query, update, and manage relational databases. Although not a programming language in the same sense as C or Pascal, SQL can be used either in formulating interactive queries or embedded in an application as instructions for handling data. The SQL standard also contains components for defining, altering, controlling, and securing data.

SVC *See* switched virtual circuit (SVC).

Switched Multimegabit Data Services (SMDS) A high-speed, switched-packet service that can provide speeds of up to 34 Mbps.

switched virtual circuit (SVC) A logical connection between end computers that uses a specific route across the network. Network resources are dedicated to the circuit, and the route is maintained until the connection is terminated. These are also known as point-to-multipoint connections. *See also* virtual circuit.

switching *See* packet switching.

symmetric multiprocessing (SMP) SMP systems, such as Windows NT Server, use any available processor on an as-needed basis. With this approach, the system load. and application needs can be distributed evenly across all available processors.

synchronous A form of communication that relies on a timing scheme coordinated between two devices to separate groups of bits and transmit them in blocks called frames. Special characters are used to begin the synchronization and check its accuracy periodically. Because the bits are sent and received in a timed, controlled (synchronized) fashion, start and stop bits are not required. Transmission stops at the end of one transmission and starts again with a new one. It is a start/stop approach, and more efficient than asynchronous transmission. If an error occurs, the synchronous error detection and correction scheme implements a retransmission. However, because more sophisticated technology and equipment is required to transmit synchronously, it is more expensive than asynchronous transmission.

Synchronous Data Link Control (SDLC) The data link (data transmission) protocol most widely used in networks conforming to IBM's SNA. SDLC is a communications guideline that defines the format in which information is transmitted. As its name implies, SDLC applies to synchronous transmissions. SDLC is also a bit-oriented protocol and organizes information in structured units called frames.

Synchronous Optical Network (SONET) A fiber-optic technology that can transmit data at more than one gigabit per second. Networks based on this technology are capable of delivering voice, data, and video. SONET is a standard for optical transport formulated by the Exchange Carriers Standards Association (ECSA) for the ANSI.

Systems Network Architecture (SNA) A widely used communication framework developed by IBM to define network functions and establish standards for enabling its different models of computers to exchange and process data. SNA is a design philosophy that separates network communication into five layers. Each layer, like those in the similar ISO/OSI model, represents a graduated level of function moving upward from physical connections to applications software.

SYSVOL A shared directory that stores the server copy of the domain's public files, which are replicated among all domain controllers in the domain.

T

T1 line A high-speed communications line that can handle digital communication and Internet access at a rate of 1.544 Mbps (megabits per second).

T1 service The standard digital line service. It provides transmission rates of 1.544 Mbps and can carry both voice and data.

tap A connection to a network. This usually refers specifically to a connection to a cable.

T connector A T-shaped coaxial connector that connects two thinnet Ethernet cables while supplying an additional connector for a network interface card.

TCP *See* Transmission Control Protocol (TCP).

TCP/IP *See* Transport Control Protocol/ Internet Protocol (TCP/IP).

TDI *See* transport driver interface (TDI).

TDR *See* time-domain reflectometer (TDR).

Technet *See* Microsoft Technical Information Network (TechNet).

Telnet The command and program used to log in from one Internet site to another. The Telnet command and program brings the user to the login prompt of another host.

terabyte *See* byte.

terminator A resistor used at each end of an Ethernet cable to ensure that signals do not reflect back and cause errors. It is usually attached to an electrical ground at one end. *See also* signal bounce.

terminator resistance The level of resistance in a terminator, measured in ohms. It must match the network architecture specification. For example, Ethernet using RG-58 A/U thinnet cable requires a 50-ohm resistor in the terminator. Terminating resistance that does not match the specifications can cause the network to fail. *See also* ohm.

thicknet (standard Ethernet) A relatively rigid coaxial cable about 0.5-inch in diameter. Typically, thicknet is used as a back-bone to connect several smaller thinnet-based networks because of its ability to support data transfer over longer distances. Thicknet can carry a signal for 500 meters (about 1640 feet) before needing a repeater.

thinnet (ThinWire Ethernet) A flexible coaxial cable about 0.25-inch thick. It is used for relatively short-distance communication and is fairly flexible to facilitate routing between computers. Thinnet coaxial cable can carry a signal up to approximately 185 meters (about 607 feet) before needing a repeater.

throughput A measure of the data transfer rate through a component, connection, or system. In networking, throughput is a good indicator of the system's total performance because it defines how well the components work together to transfer data from one computer to another. In this case, the throughput would indicate how many bytes or packets the network could process per second.

ticket A set of identification data for a security principle, issued by a domain controller for purposes of user authentication. Two forms of tickets in Windows 2000 are ticket-granting tickets (TGTs) and service tickets.

time-domain reflectometer (TDR) A trouble-shooting tool that sends sonar-like pulses along a cable looking for any kind of a break, short, or imperfection that might affect performance. If the pulse finds a problem, the TDR analyzes it and displays the result. A good TDR can locate a break to within a few feet of the actual separation in the cable.

Time-to-Live (TTL) A timer value included in packets sent over TCP/IP-based networks that tells the recipients how long to hold or use the packet or any of its included data before expiring and discarding the packet or data. For DNS, TTL values are used in resource records within a zone to determine how long requesting clients should cache and use this information when it appears in a query response answered by a DNS server for the zone.

token A predetermined formation of bits that permits a network device to communicate with the cable. A computer cannot transmit unless it has possession of the token. Only one token at a time can be active on the network, and the token can travel in only one direction around the ring. *See also* token passing, Token Ring network.

token passing A media access control method in a Token Ring network in which a data frame, called a token, is passed from one station to the next around the ring. *See also* token, Token Ring network.

Token Ring network A network in which computers are situated on a continuous network loop through which a token is passed from one computer to the next. Computers are centrally connected to a hub called a Multistation Access Unit (MAU) and are wired in a star configuration. Computers use a token to transmit data and must wait for a free token in order to transfer data. *See also* token, token passing.

TokenTalk An expansion card that allows a Macintosh II to connect to an 802.5 Token Ring network.

tone generator and tone locator Standard wiring tools used for troubleshooting. The tone generator is used to apply an alternating or continuous tone signal to a cable or conductor and is attached to one end of the cable. A matching tone locator is used to detect the correct cable at the other end of the run. These tools are also referred to as a "fox and hound."

tone locator *See* tone generator and tone locator.

topology The arrangement or layout of computers, cables, and other components on a network. Topology is the standard term that most network professionals use when referring to the network's basic design.

tracert A Trace Route command-line utility that shows every router interface through which a TCP/IP packet passes on its way to a destination.

trailer One of the three sections of a packet component. The exact content of the trailer varies depending on the protocol, but it usually includes an error-checking component (CRC).

transceiver A device that connects a computer to the network. The term is derived from transmitter/receiver; thus, a transceiver is a device that receives and transmits signals. It switches the parallel data stream used on the computer's bus into a serial data stream used in the cables connecting the computers.

Transmission Control Protocol (TCP) The TCP/IP protocol for sequenced data. *See also* Transport Control Protocol/Internet Protocol (TCP/IP).

Transport Control Protocol/Internet Protocol

(TCP/IP) An industry standard suite of protocols providing communications in a heterogeneous environment. In addition, TCP/IP provides a routable, enterprise networking protocol and access to the Internet and its resources. It is a transport layer protocol that actually consists of several other protocols in a stack that operates at the session layer. Most networks support TCP/IP as a protocol.

transport driver interface (TDI) An interface that works between the file-system driver and the transport protocols, allowing any protocol written to TDI to communicate with the file-system drivers.

transport layer The fourth layer of the OSI reference model. It ensures that messages are delivered error free, in sequence, and with-out losses or duplications. This layer repackages messages for efficient transmission over the network. At the receiving end, the transport layer unpacks the messages, reassembles the original

messages, and sends an acknowledgment of receipt. *See also* Open Systems Interconnection (OSI) reference model.

transport protocols Protocols that provide for communication sessions between computers and ensure that data is able to move reliably between computers.

"Trojan horse" virus A type of virus that appears to be a legitimate program that might be found on any system. The Trojan horse virus can destroy files and cause physical damage to disks.

trunk A single cable, also called a backbone, or segment.

trust relationship Trust relationships are links between domains that enable pass-through authentication, in which a user has only one user account in one domain, yet can access the entire network. User accounts and global groups defined in a trusted domain can be given rights and resource permissions in a trusting domain even though those accounts do not exist in the trusting domain's database. A trusting domain honors the logon authentication of a trusted domain.

TTL (Time-to-Live) *See* Time-to-Live (TTL).

twisted-pair cable A cable that consists of two insulated strands of copper wire twisted together. A number of twisted-wire pairs are often grouped together and enclosed in a protective sheath to form a cable. Twisted-pair cable can be shielded or unshielded. Unshielded twisted-pair cable is commonly used for telephone systems. *See also* shielded twisted-pair (STP) cable, unshielded twisted-pair (UTP) cable.

U

UART *See* universal asynchronous receiver transmitter (UART).

UDP *See* User Datagram Protocol (UDP).

Uniform Resource Locator (URL) Provides the hypertext links between documents on the World Wide Web (WWW). Every resource on the Internet has its own location identifier, or URL, that specifies the server to access as well as the access method and the location. URLs can use various protocols including FTP and HTTP.

UNC (Universal Naming Convention) *See* Universal Naming Convention (UNC).

uninterruptible power supply (UPS) A device connected between a computer or another piece of electronic equipment and a power source, such as an electrical outlet. The UPS ensures that the electrical flow to the computer is not interrupted because of a blackout and, in most cases, protects the computer against potentially damaging events such as power surges and brownouts. Different UPS models offer

different levels of protection. All UPS units are equipped with a battery and loss-of-power sensor. If the sensor detects a loss of power, it immediately switches over to the battery so that users have time to save their work and shut off the computer. Most higher-end models have features such as power filtering, sophisticated surge protection, and a serial port so that an operating system capable of communicating with a UPS (such as Windows NT) can work with the UPS to facilitate automatic system shutdown.

universal asynchronous receiver transmitter (UART) A module, usually composed of a single integrated circuit, that contains both the receiving and transmitting circuits required for asynchronous serial communication. Two computers, each equipped with a UART, can communicate over a simple wire connection. The operation of the sending and receiving units are not synchronized by a common clock signal, so the data stream itself must contain information about when packets of information (usually bytes) begin and end. This information about the beginning and ending of a packet is provided by. the start and stop bits in the data stream. A UART is the most common type of circuit used in personal-computer modems.

Universal Naming Convention (UNC) The standard used for a full Windows 2000 name of a resource on a network. It conforms to the *server**share* syntax, where servername is the name of the server and sharename is the name of the shared resource. UNC names of directories or files can also include the directory path under the share name, with the following syntax:*server**share**directory*\ *filename*.

Universal Serial Bus (USB) A serial bus with a data transfer rate of 12 megabits per second (Mbps) for connecting peripherals to a microcomputer. USB can connect up to 127 peripheral devices to the system through a single, general-purpose port. This is accomplished by daisy chaining peripherals together. USB is designed to support the ability to automatically add and configure new devices and the ability to add such devices without having to shut down and restart the system.

unshielded twisted-pair (UTP) cable A cable with wires that are twisted around each other with a minimum number of twists per foot. The twists reduce signal interference between the wires. The more twists per foot, the greater the reduction in interference (crosstalk). This cable is similar to shielded twisted-pair (STP) cable, but lacks the insulation or shielding found in STP cable.

UPS *See* uninterruptible power supply (UPS).

URL *See* Uniform Resource Locator (URL).

USB *See* Universal Serial Bus (USB).

user account Consists of all of the information that defines a user on a network. This includes the user name and password required for the user to log on, the groups in which the user account has membership, and the rights and permissions the user has for using the system and accessing its resources.

User Datagram Protocol (UDP) A connectionless protocol, responsible for end-to- end data transmission.

user groups Groups of users who meet online or in person to discuss installation, administration, and other network challenges for the purpose of sharing and drawing on each other's expertise in developing ideas and solutions.

UTP *See* unshielded twisted-pair (UTP) cable.

V

vampire tap (piercing tap transceiver) An Ethernet transceiver housed in a clamp-like device with sharp metal prongs that "bite" through thicknet cable insulation and make contact with the copper core. The transceiver's DIX (DB15) connector provides an attachment for an AUI cable that runs from the transceiver to either the computer or a hub or repeater. Along thick coaxial cable that includes bands spaced 2.5 meters (8 feet) apart, a vampire tap is inserted into each band; an AUI, DIX, or DB15 connector then attaches a cable from the tap to the computer or other device to be added to the Ethernet network.

virtual circuit A series of logical connections between a sending computer and receiving computer. The connection is made after both computers exchange information and agree on communication parameters that establish. and maintain the connection, including maximum message size and path. Virtual circuits incorporate communication parameters such as acknowledgments, flow control, and error control to ensure reliability. They can be either temporary, lasting only as long as the conversation, or permanent, lasting as long as the users keep the communication channel open.

Virtual Private Network (VPN) A set of computers on a public network such as the Internet that communicate among themselves using encryption technology. In this way their messages are safe from being intercepted and understood by unauthorized users. VPNs operate as if the computers were connected by private lines.

virus Computer programming, or code, that hides in computer programs or on the boot sector of storage devices such as hard-disk drives and floppy-disk drives. The primary purpose of a virus is to reproduce itself as often as possible; a secondary purpose is to disrupt the operation of the computer or the program.

voltmeter *See* digital voltmeter (DVM).

volume set A collection of hard-disk partitions that are treated as a single partition, thus increasing the disk space available in a single drive letter. Volume sets are created by combining between 2 and 32 areas of unformatted free space on one or more physical drives. These spaces form one large logical volume set which is treated like a single partition.

W

wide area network (WAN) A computer network that uses long-range telecommunication links to connect networked computers across long distances.

winipcfg A diagnostic command specific to Microsoft Windows 95 and 98. Although this graphical user interface (GUI) utility duplicates the functionality of ipconfig, its GUI makes it easier to use. *See also* ipconfig.

wireless bridge A component that offers an easy way to link buildings without using cable.

wireless concentrator A component that acts as a transceiver to send and receive signals while communicating with network interface cards.

wireless network An emerging networking option consisting of wireless components that communicate with a network that uses cables in a mixed-component network called a hybrid.

workgroup A collection of computers grouped for sharing resources such as data and peripherals over a LAN. Each workgroup is identified by a unique name. *See also* domain, peer-to-peer network.

World Wide Web (the Web, or WWW) The Internet multimedia service that contains a vast store-house of hypertext documents written in HTML. *See also* Hypertext Markup Language (HTML).

WORM *See* Write-Once Read-Many (WORM).

Write-Once Read-Many (WORM) Any type of storage medium to which data can be written only once, but can be read any number of times. Typically, this is an optical disc whose surface is permanently etched using a laser, in order to record information.

X

X.25 A recommendation published by the CCITT that defines the connection between a terminal and a packet-switching network. A packet-switching network routes packets whose contents and format are controlled. standards such as those defined in the X.25 recommendation. X.25 incorporates three definitions: the electrical connection between the terminal and the network, the transmission or link-access protocol, and the implementation of virtual circuits between network users. Taken together, these definitions specify a synchronous, full-duplex, terminal-to-network connection. Packets transmitted in such a network can contain either data or control commands. Packet format, error control, and other features are equivalent to portions of the HDLC protocol defined by the ISO. X.25 standards are related to the lowest three levels of the OSI reference model.

X.400 A CCITT protocol for international e-mail transmissions.

X.500 A CCITT protocol for file and directory maintenance across several systems.

XNS (Xerox Network System) Protocol developed by Xerox for its Ethernet LANs.

Z

Zones Logical groupings of users and resources in an AppleTalk network.

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q-R

S

T

U

V

W

X–Z